Problems related to lattice points in the plane

Shaunna Plunkett-Levin

School of Mathematics
Cardiff University
October 2011

This thesis is submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy.

Summary

In the first part of this research we find an improvement to Huxley and Konyagin's current lower bound for the number of circles passing through five integer points. The improved lower bound is the conjectured asymptotic formula for the number of circles passing through five integer points. We generalise the result to circles passing through more than five integer points, giving the main theorem.

Theorem. *Let $m \geq 4$ be a fixed integer. Let $W_m(R)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with radius $r \leq R$. There exists a polynomial $w(x)$ such that*

$$W_m(R) \geq \frac{4^m}{m!} R^2 \; w(\log R)(1 + o(1))$$

where $w(x)$ is an explicit polynomial of degree $2^{m-1} - 1$.

In the second part of the research we consider questions linked to the distribution of different configurations of integer points of the circle passing through the unit square. We show that different configurations of points are distributed uniformly throughout the unit square for circles of fixed radius. Results are obtained by looking at the distribution of the crossing points of circles, where the circles form the boundaries of domains. The domain of a configuration is the set of possible positions of the centre of the circle within the configuration. We choose a rectangle within the unit square and then count the number of regions of the rectangle which are formed by domain boundaries.

Theorem. *The number of domains which meet a given rectangle with side lengths α and β is*

$$4\pi R^2 \alpha\beta + O\left(R^{\kappa+1}(\log R)^{\lambda}\right),$$

where $\kappa = 131/208$ and $\lambda = 18627/8320$.

Acknowledgements

I would like to acknowledge the financial support provided to me by the School of Mathematics at Cardiff University, and by my husband, Alex Levin.

I could not have completed this work without the help, support, guidance and patience of Professor Martin Huxley. I am incredibly grateful for his advice and wisdom.

I would also like to thank Dr Jovisa Zunic, for suggesting the use of Xfig software to draw diagrams and for providing some examples of diagrams drawn in Xfig. My colleagues, Dr Nigel Watt and Dr Matthew Lettington, have also been helpful in answering my questions and providing advice.

I need to thank Alex Levin for encouraging me and being there for me throughout my studies, and indeed throughout our life together. Thank you also to my parents, Kevin and Glynis Plunkett, for their care, support and encouragement. In particular, thanks to my Mum, Glynis Plunkett, for looking after my daughter, Freda Levin, to ensure that I finished this work.

I dedicate this work to my daughter Freda; who delayed my completion, drooled on my drafts, and ensured that never has one page of mathematics been as well-loved, chewed, ripped and crinkled as page 81.

Contents

List of Figures

Part I

Counting the number of cyclic polygons with five or more integer point vertices

Chapter 1

Introducing cyclic polygons and the function $r(n)$

1.1 History of the problem

The key work in the history of the problem considered in the first part of this project is that of Ramanujan concerning "the representation of a number as the sum of s squares, s being any positive integer" [32]. Ramanujan set $s = 2$ and looked at the sum of two squares problem, a problem dating back to the work of Gauss [9]. In [31] Ramanujan gave formulae concerned with both the sum of squares function and the divisor function. However, Ramanujan did not give proofs of these formulae as he believed they did not "involve the use of any new ideas". Both of Ramanujan's papers [31, 32] are reproduced in the collection of his papers [33].

B.M. Wilson [42], in a paper entitled "Proofs of some formulae enunciated by Ramanujan", proved many of the formulae given by Ramanujan. Wilson's paper was mainly concerned with moments of the divisor function, and it proved in full Ramanujan's results on the divisor function. Wilson also outlined proofs of Ramanujan's other results. The most interesting aspect of Wilson's paper in terms of this research project is Wilson's prediction of the existence of results for powers of the function $r(n)$ analogous to the results proved by Wilson for the divisor function. The function $r(n)$ is the arithmetic function counting the number of integer solutions of $x^2 + y^2 = n$, where $x > 0$ and $y \geq 0$.

Ramanujan used the standard notation of $\zeta(s)$ for the Riemann zeta function; γ for Euler's constant; and ϵ for any small positive number. The

main result of Ramanujan's that we are interested in is his expression for the sum between 1 and n of $r^2(n)$.

Result (Ramanujan's result)**.** *If*

$$\left(\frac{1}{2}+q+q^4+q^9+q^{16}+\ldots\right)^2=\sum_1^\infty r(n)q^n$$

so that

$$\zeta(s)\eta(s)=\sum_1^\infty r(n)n^{-s},$$

where

$$\eta(s)=1^{-s}-3^{-s}+5^{-s}-7^{-s}+\ldots,$$

then

$$\frac{\zeta^2(s)\eta^2(s)}{(1+2^{-s})\zeta(2s)}=1^{-s}r^2(1)+2^{-s}r^2(2)+3^{-s}r^2(3)+\ldots,$$

and

$$r^2(1)+r^2(2)+r^2(3)+\ldots+r^2(n)=\frac{n}{4}(\log n+c)+O\left(n^{3/5+\epsilon}\right),$$

where

$$c=4\gamma-1+\frac{1}{3}\log 2-\log\pi+4\log\Gamma\left(\frac{3}{4}\right)-\frac{12}{\pi^2}\zeta'(2).$$

The order of magnitude term $O(n^{3/5+\epsilon})$ has been subsequently improved. The best known order of magnitude term is currently that of Huxley, which gives $O(n^{131/208+\epsilon})$, proved in [17]. The conjectured order of magnitude term is $O(n^{1/2+\epsilon})$ [11].

Wilson states that

$$\sum_{n=1}^\infty n^{-s}r(n)=4^k\left(1-2^{-s}\right)^{2^{(k-1)}-1}\left\{\zeta(s)\eta(s)\right\}^{2^{(k-1)}}\phi(s),$$

where $\eta(s)$ is as before; $\phi(s)$ is absolutely convergent for $\mathrm{Re}(s)=\sigma>1/2$; and k denotes a positive integer.

This can be reformulated, as in the work of Huxley and Konyagin [20], to give

Wilson's Proposition. *For each integer $m\geq 1$, there are constants b_m,*

$b_m = 2^{m-1} - 1$, *and* c_m, *such that as* $N \to \infty$, *we have*

$$\sum_{n \leq N} r^m(n) = (c_m + o(1))N(\log N)^{b_m}.$$

The work of Huxley and Konyagin [20] considers the question "Among the circles drawn through three distinct integer points in the plane, are circles which pass through four or more points rare?" This arose from the investigation by Huxley and Žunić [22,25] of the configurations of integer points in convex plane sets. Huxley and Konyagin [20] study families of circles passing through three, four and five integer points finding upper and lower bounds.

Using the notation of [20], let $P_m(R)$ denote the number of sets of m distinct integer points lying on a circle of radius r with $r \leq R$. For sufficiently large R, Huxley and Konyagin have bounded $P_m(R)$ for $m = 3, 4, 5$.

$$P_3(R) = \pi^2 R^4 + O(R^{2+\kappa}(\log R)^{\lambda}),$$

where $\kappa = 131/208$ and $\lambda = 18627/8320$. We will use these values of κ and λ throughout this research.

$$P_4(R) = \frac{32(3+\sqrt{2})}{21\zeta(3)}\zeta\left(\frac{3}{2}\right)L\left(\frac{3}{2},\chi\right)R^3 + O(R^{76/29+\epsilon}),$$

where $\epsilon > 0$ and $L(s,\chi)$ is the Dirichlet L-function formed with the non-trivial character mod 4. For $P_5(R)$ with $\epsilon > 0$, the current bounds are

$$cR^2 \log R \leq P_5(R) \leq C(5,\epsilon)R^{76/29+\epsilon}.$$

We begin this research with an improvement to Huxley and Konyagin's current lower bound for the number of circles passing through five integer points, which is identically the lower bound for the number of circles in which cyclic polygons with five integer point vertices can be inscribed. The improved lower bound is the conjectured asymptotic formula for the number of circles passing through five integer points. We also generalise our results to circles passing through more than five integer points.

The first result found was a more precise form of Wilson's Proposition for $m \geq 3$. We then established the conjectured asymptotic formula for the number of cyclic polygons with m integer vertices, for each $m \geq 3$, which have circumcentre at the origin and circumradius at most $\sqrt{N}$. Next,

we restricted this result to $r^*(n,q)$, the arithmetic function that counts the number of integer solutions of $x^2+y^2=n$ with $x>0$, $y\geq 0$ and highest common factor $(x,y,q)=1$.

Our next result was a lemma giving a way of establishing a lower bound for the number of cyclic polygons with five or more integer point vertices. We then restricted the size of the circumradius in this lemma to be less than or equal to R and thus we obtained a theorem giving a lower bound for the number of m-sided cyclic polygons with radius up to size R. This is the conjectured asymptotic formula for the number of circles passing through five or more integer points.

1.2 Notation

We use the standard notation $s=\sigma+it$ where $\sigma=\mathrm{Re}(s)$ and $t=\mathrm{Im}(s)$. This is associated with our use of the Riemann zeta function $\zeta(s)$ where

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}.$$

We define $L(s,\chi)$ as the Dirichlet L-function formed with the non-trivial character mod 4. We also use the Dedekind zeta function $Z(s)$, which is a product of the Riemann zeta function and Dirichlet L-function, so that $Z(s)=\zeta(s)L(s,\chi)$. When the constants κ and λ appear, they take the values $\kappa=131/208$ and $\lambda=18627/8320$, values obtained by Huxley in [17].

When there is an exponent of ϵ in an order of magnitude term, the exponent ϵ may be taken arbitrarily small and positive, but the constant implied in the O-symbol will depend on ϵ. The Vinogradov symbol $f(x)\ll g(x)$ as $x\to\infty$ means $f(x)=O(g(x))$ as $x\to\infty$, where $g(x)$ is positive for all large x. Similarly $f(x)\gg g(x)$ as $x\to\infty$ means that $g(x)=O(f(x))$ as $x\to\infty$, where $f(x)$ and $g(x)$ are positive for all large x. The symbol $\asymp$ means asymptotically equal to, that is $A\ll B\ll A$, with implied constant ϵ again.

Chapter 2

Sums of powers of the function $r(n)$ and asymptotic formulae for the number of cyclic polygons of fixed radius with m integer point vertices

2.1 Theorem 1 on the sums of powers of the function $r(n)$

Theorem 1. *Let $m \geq 3$ be a fixed integer, and $r(n)$ be the arithmetic function counting the number of integer solutions of $x^2+y^2 = n$, with $x > 0$ and $y \geq 0$, then, as $N \to \infty$,*

$$\sum_{n \leq N} r^m(n) = N \; P_m(\log N) + O(N^{\Phi+\epsilon}), \tag{2.1}$$

where $P_m(x)$ is a polynomial of degree $b = 2^{m-1} - 1$, and Φ is an exponent less than 1. The exponent ϵ and the constant implied in the O symbol follow the conventions given in Section 1.2.

To define the exponent Φ in the error term of Theorem 1 we need to introduce the exponent ϕ. The exponent ϕ is known for the size of the

Riemann zeta function [37],

$$\zeta\left(\frac{1}{2}+it\right)=O\left(t^{\phi+\eta}\right)$$

for all $\eta>0$ as $t\to+\infty$. By Huxley's estimate [18], we take $\phi=32/205$. The exponent Φ is then given by

$$\Phi=\frac{(4b-4)\phi+1}{(4b-4)\phi+2}, \tag{2.2}$$

where $b=2^{m-1}-1$ is the degree of the polynomial $P_m(x)$.

2.2 Proof of Theorem 1 on sums of powers of the function $r(n)$

We begin our proof by writing the Dirichlet series $F(s)$ for $r^m(n)$ as an Euler product,

$$F(s)=\sum_{n=1}^{\infty}\frac{r^m(n)}{n^s}=\prod_{p\text{ prime}}\left(1+\frac{r^m(p)}{p^s}+\frac{r^m(p^2)}{p^{2s}}+\cdots\right). \tag{2.3}$$

We consider values of $r(n)$ for $n=p^k$, with p prime. We have

$$r(p^k)=\begin{cases}1 & \text{p}=2\\ k+1 & p\equiv 1 \bmod 4,\\ 1 & p\equiv 3 \bmod 4,\ k \text{ even},\\ 0 & p\equiv 3 \bmod 4,\ k \text{ odd}.\end{cases}$$

Then, for m a positive integer, we have

$$r^m(p^k)=\begin{cases}1 & p=2\\ (k+1)^m & p\equiv 1 \bmod 4,\\ 1 & p\equiv 3 \bmod 4,\ k \text{ even},\\ 0 & p\equiv 3 \bmod 4,\ k \text{ odd}.\end{cases} \tag{2.4}$$

We recall that $r(n)$ is the arithmetic function counting the number of integer solutions of $x^2+y^2=n$, with $x>0$ and $y\geq 0$, and we show that

$r(n)$ is multiplicative. We define $\chi(d)$ for $d > 0$ as $\chi(d) = 0$ when $2|d$ and $\chi(d) = (-1)^{(d-1)/2}$ when $2 \nmid d$, and write

$$r(n) = \sum_{d|n} \chi(d).$$

Since $\chi(d)$ is multiplicative [13], $r(n)$ will also be multiplicative. The multiplicative property of $r(n)$ means we can substitute the values from (2.4) into (2.3) to find

$$F(s) = G\left(\frac{1}{2^s}\right) \prod_{p \equiv 1 \bmod 4} H\left(\frac{1}{p^s}\right) \prod_{p \equiv 3 \bmod 4} G\left(\frac{1}{p^{2s}}\right). \tag{2.5}$$

Here $G(x)$ and $H(x)$ are infinite series that can be expressed as rational functions,

$$\begin{aligned} G(x) &= 1 + x + x^2 + \cdots = \frac{1}{1-x}, \\ H(x) &= 1 + 2^m x + 3^m x^2 + 4^m x^3 + \cdots = \frac{1}{(1-x)^{m+1}} \sum_{k=1}^{m} A(m,k) x^{k-1}, \end{aligned} \tag{2.6}$$

the defining property of the Eulerian numbers $A(m,k)$ given in (2.47).

The Dirichlet series for $r^m(n)$ can be written in terms of the Dedekind zeta function $Z(s) = \zeta(s)L(s,\chi)$, the product of the Riemann zeta function and Dirichlet L-function, so that

$$F(s) = \sum_{n=1}^{\infty} \frac{r^m(n)}{n^s} = Z^{b+1}(s) E(s). \tag{2.7}$$

We then equate (2.5) and (2.7), our two expressions for the Dirichlet series of $r^m(n)$, to obtain

$$\begin{aligned} E(s) = &\left(1 - \frac{1}{2^s}\right)^b \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^{2s}}\right)^b \\ &\prod_{p \equiv 1 \bmod 4} \left(1 - \frac{1}{p^s}\right)^{A(m,2)} \sum_{k=1}^{m} A(m,k) p^{s(1-k)}. \end{aligned} \tag{2.8}$$

The product E in (2.46) is $E(1)$ in the notation (2.8).

We need to find an analytic continuation of $E(s)$. We do this by compar-

ing $E(s)$ to $\zeta(2s)$ and $L(2s,\chi)$ as infinite products of primes. We write

$$E(s) = \frac{J(s)}{\zeta^{j_1}(2s) L^{j_2}(2s,\chi)}, \tag{2.9}$$

where the exponents j_1 and j_2 are found from $b = 2^{m-1} - 1$ and

$$d = 2^{m-1}(2^m + 1) - 3^m, \tag{2.10}$$

with

$$\begin{aligned} j_1 &= \frac{d+b}{2} = 2^{m-1}(2^{m-1}+1) - \frac{1}{2}(3^m+1), \\ j_2 &= \frac{d-b}{2} = 2^{2(m-1)} + \frac{1}{2}(1-3^m). \end{aligned}$$

The residual factor $J(s)$ of the expression for $E(s)$ given in (2.9) is

$$J(s) = A(2) \prod_{p \equiv 1 \bmod 4} B(p) \prod_{p \equiv 3 \bmod 4} C(p),$$

where $A(2)$ is a rational function in $1/2^s$, with poles on $\mathrm{Re}(s) = 0$, and for calculable constants β, and γ,

$$B(p) = 1 + \frac{\beta}{p^{3s}} + \cdots, \qquad C(p) = 1 + \frac{\gamma}{p^{3s}} + \cdots .$$

The Dirichlet series for $\log J(s)$ converges absolutely for $\sigma > 1/3$ by comparison with the series $\zeta(3\sigma)$. However, at $s = 1/2$, $\zeta(2s)$ has a pole, whilst the series for $L(2s,\chi)$ converges for $\sigma > 0$. Hence $E(s)$ can be continued analytically to $\sigma > 1/2$.

We now consider the size of $E(s)$,

$$|E(s)| = \frac{|J(s)|}{|\zeta(2s)|^{j_1} \, |L(2s,\chi)|^{j_2}}.$$

The series $\log J(s)$, and thus $|J(s)|$, is uniformly bounded for $\sigma \geq 1/2$, with $|J(s)| < \tilde{J}$, for some constant $\tilde{J}$. We estimate $|1/\zeta(2s)|$ and $1/|L(2s,\chi)|$. Using the Möbius function, $\mu(n)$, we find

$$\frac{1}{|\zeta(2s)|} = \left| \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{2s}} \right| \leq \sum_{n=1}^{\infty} \frac{1}{|n^{2s}|} = \sum_{n=1}^{\infty} \frac{1}{n^{2\sigma}} = \zeta(2\sigma),$$

and similarly

$$\frac{1}{|L(2s,\chi)|} = \left|\sum_{n=1}^{\infty} \frac{\mu(n)\chi(n)}{n^{2s}}\right| \leq \sum_{n=1}^{\infty} \frac{1}{|n^{2s}|} = \sum_{n=1}^{\infty} \frac{1}{n^{2\sigma}} = \zeta(2\sigma).$$

Hence, for $\sigma > 1/2$, we have the inequalities

$$\frac{1}{|\zeta(2s)|} \leq \zeta(2\sigma), \qquad \frac{1}{|L(2s,\chi)|} \leq \zeta(2\sigma),$$

and

$$|E(s)| = \frac{|J(s)|}{|\zeta(2s)|^{j_1}\,|L(2s,\chi)|^{j_2}} \leq \tilde{J}\,(\zeta(2\sigma))^{j_1+j_2} = \tilde{J}\zeta^d(2\sigma),$$

in the notation (2.10). We need several lemmas to continue the proof of Theorem 1.

2.3 Truncating the Mellin transform

We explain the standard method of truncating the contour integral which defines the Mellin transform for a single term of a Dirichlet series. A variant of our method can be found in Montgomery and Vaughan (chapter 5, [30]).

Lemma 2.1. *Let $\eta > 0$ be given, then*

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} \left(\frac{x}{n}\right)^s \frac{\mathrm{d}s}{s} = \begin{cases} 1 + O\left(\left(\frac{x}{n}\right)^{1+\eta} \frac{1}{T\log(x/n)}\right) & \text{if } n < x, \\ O\left(\left(\frac{x}{n}\right)^{1+\eta} \frac{1}{T\log(n/x)}\right) & \text{if } n > x. \end{cases}$$

Proof. Let C be a closed contour, then

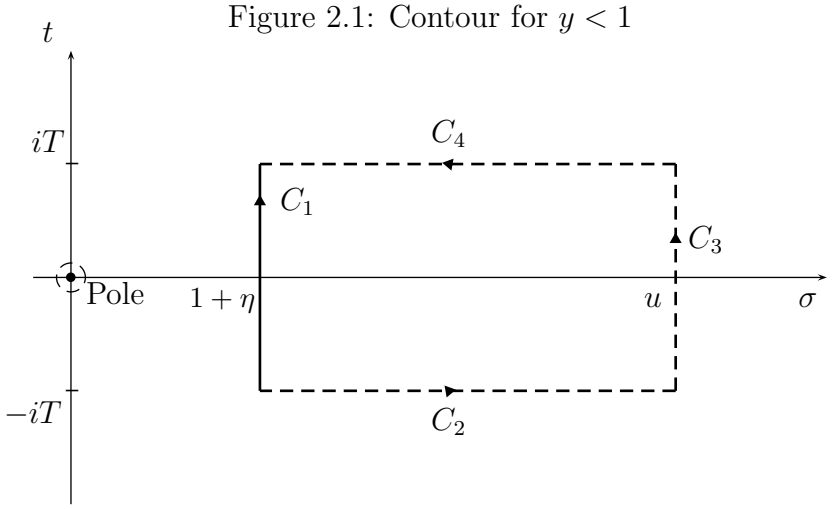
$$\frac{1}{2\pi i}\oint_C f(s)\,\mathrm{d}s = \begin{cases} 1 & \text{if the origin is inside } C, \\ 0 & \text{if the origin is outside } C. \end{cases}$$

Let $f(s) = y^s/s$, with $y = x/n$, and $y > 0$. Then $f(s)$ has a pole at $s = 0$ with residue $y^0 = 1$.

We consider the integral along the line segment C_1, which runs from $1+\eta+iT$ to $1+\eta-iT$,

$$\frac{1}{2\pi i}\int_{C_1} f(s)\,\mathrm{d}s = \frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} f(s)\,\mathrm{d}s.$$

Figure 2.1: Contour for $y < 1$



In order to have a closed contour C, we add line segments C_2, C_3 and C_4 to the line segment C_1. We have two cases to consider, $y > 1$ or $y < 1$, which influence our choice of line segments C_2, C_3 and C_4. For $y > 1$, as $\sigma = \mathrm{Re}(s) \to -\infty$, $y^s \to 0$. For $y < 1$, as $\sigma \to +\infty$, $y^s \to 0$.

For $y < 1$, we set $u > 1 + \eta$, then C_2 is the line segment running from $1 + \eta - iT$ to $u - iT$. C_3 is the line segment running from $u - iT$ to $u + iT$, and C_4 is the line segment running from $u + iT$ to $1 + \eta + iT$. Figure 2.1 shows the contour used for $y < 1$, with

$$\int_{C_1} f(s)\,\mathrm{d}s = \int_{C_2} f(s)\,\mathrm{d}s + \int_{C_3} f(s)\,\mathrm{d}s + \int_{C_4} f(s)\,\mathrm{d}s. \tag{2.11}$$

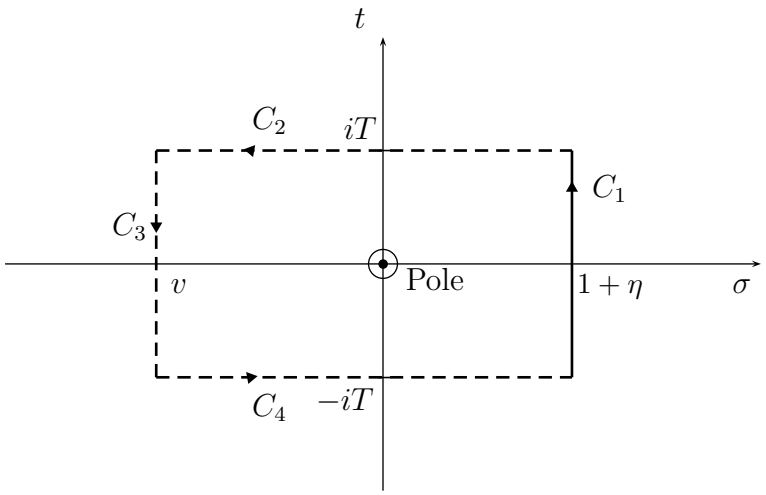
For $y > 1$, set $v < 0$, and then C_2 is the line segment running from $1 + \eta + iT$ to $v + iT$. C_3 is the line segment running from $v + iT$ to $v - iT$, and C_4 is the line segment running from $v - iT$ to $1 + \eta - iT$. Figure 2.2 shows the contour for $y > 1$, with

$$\frac{1}{2\pi i} \oint_{C_1+C_2+C_3+C_4} f(s)\,\mathrm{d}s = 1. \tag{2.12}$$

In both of our cases we find that $|1/s|$, y^s, and the function $f(s) = y^s/s$ are small along C_3. We also have $T > 0$, so that $|1/s| \leq 1/T$ along C_2 and C_4, with $|y^s|$ decreasing away from C_1 in both of our cases.

We begin with the case $y < 1$, equivalent to $n < x$. Along C_2, we have

Figure 2.2: Contour for $y > 1$



the estimate of $|f(s)|$,

$$|f(s)| = \left|\frac{y^s}{s}\right| = \left|\frac{e^{(\sigma - iT)\log y}}{\sigma - iT}\right| \leq \frac{e^{\sigma \log y}}{T} = \frac{y^\sigma}{T},$$

and we use the range of values of σ along C_2, $1 + \eta \leq \sigma \leq u$, to get

$$\left|\frac{1}{2\pi i}\int_{C_2} f(s)\,\mathrm{d}s\right| \leq \int_{1+\eta}^{u} \frac{y^\sigma}{T} \leq \frac{y^{1+\eta}}{T\log(1/y)}. \tag{2.13}$$

Similarly along C_4, we estimate $|f(s)| \leq y^\sigma/T$, and our estimate for the integral along C_4 is

$$\left|\frac{1}{2\pi i}\int_{C_4} f(s)\,\mathrm{d}s\right| \leq \frac{y^{1+\eta}}{T\log(1/y)}. \tag{2.14}$$

Along C_3, we have an interval of length $2T$, and we can estimate $|f(s)|$ as $|f(s)| \leq y^u/u$. We find

$$\left|\frac{1}{2\pi i}\int_{C_3} f(s)\,\mathrm{d}s\right| \leq 2T\ \frac{y^u}{u} \leq 0, \tag{2.15}$$

since for $y < 1$, as $u \to +\infty$, $1/u \to 0$, and $y^u \to 0$ as well.

We use the triangle inequality on (2.11) and the results of (2.13), (2.14)

and (2.15) to obtain

$$\left|\int_{C_1}\right| \leq \frac{y^{1+\eta}}{T\log(1/y)} + 0 + \frac{y^{1+\eta}}{T\log(1/y)},$$

and hence

$$\left|\frac{1}{2\pi i}\int_{C_1} f(s)\,\mathrm{d}s\right| = O\left(\frac{y^{1+\eta}}{T\log(1/y)}\right). \tag{2.16}$$

This corresponds to the result in the Lemma with $n > x$, by substituting $y = x/n$ and $f(s) = y^s/s$.

We now consider the case of $y > 1$, which corresponds to $x < n$ in the Lemma. We use (2.12), the properties of the modulus, and the triangle inequality to get

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{C_1} f(s)\,\mathrm{d}s\right| &\leq 1 + \left|\frac{1}{2\pi i}\int_{C_2+C_3+C_4} f(s)\,\mathrm{d}s\right| \\ &\leq 1 + \left|\int_{C_2} f(s)\,\mathrm{d}s\right| + \left|\int_{C_3} f(s)\,\mathrm{d}s\right| + \left|\int_{C_4} f(s)\,\mathrm{d}s\right|. \end{aligned} \tag{2.17}$$

We consider each of the integrals along C_2, C_3 and C_4 separately.

We begin with the integral along C_2. We have $|f(s)| \leq y^\sigma/T$ again, and $v \leq \sigma \leq 1+\eta$. Thus

$$\left|\int_{C_2} f(s)\,\mathrm{d}s\right| = \int_v^{1+\eta} \frac{y^\sigma}{T}\,\mathrm{d}\sigma = \frac{(y^{1+\eta} - y^v)}{T\log y}.$$

Due to the sizes of y and v respectively, we have $y^{1+\eta} - y^v \leq y^{1+\eta}$, so that

$$\left|\int_{C_2} f(s)\,\mathrm{d}s\right| \leq \frac{y^{1+\eta}}{T\log y}. \tag{2.18}$$

Likewise for the integral along C_4, we have $|f(s)| \leq y^\sigma/T$, and

$$\left|\int_{C_4} f(s)\,\mathrm{d}s\right| \leq \frac{y^{1+\eta}}{T\log y}. \tag{2.19}$$

We now look at what happens to the integral along C_3. We have

$$|f(s)| = \left|\frac{e^{(v+it)\log y}}{v+it}\right| = \frac{e^{v\log y}}{\sqrt{v^2+t^2}} \leq -\frac{1}{v}e^{v\log y} = -\frac{1}{v}y^v;$$

where the coefficient $-1/v$ is positive, since $v < 0$. The length of the inte-

grand is $2T$ so we have

$$\left|\int_{C_3} f(s)\,\mathrm{d}s\right| \le \frac{2T}{v}y^v \le 0, \tag{2.20}$$

since for $y > 1$, as $v \to -\infty$, $-2T/v \to 0$, and $y^v \to 0$.

From (2.17), with the results of (2.18), (2.19) and (2.20), we obtain

$$\left|\frac{1}{2\pi i}\int_{C_1} f(s)\,\mathrm{d}s\right| = 1 + O\left(\frac{y^{1+\eta}}{T\log y}\right). \tag{2.21}$$

This corresponds to the result in the Lemma with $n < x$, by substituting $y = x/n$ and $f(s) = y^s/s$. □

2.4 Truncating the integral

We apply the truncation of Section 2.3 to the series $F(s)$ term-by-term.

Lemma 2.2. *Let*

$$F(s) = \sum_{n=1}^{\infty} \frac{r^m(n)}{n^s}.$$

Let N be a positive integer. Set $x = N + 1/2$ and $\eta = 2/\log x$. Then

$$\sum_{n\le N} r^m(n) = \frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(s)\frac{x^s}{s}\,\mathrm{d}s + O\left(\frac{x^{1+\epsilon}\log x}{T}\right),$$

using our conventions on exponents ϵ, and remainder terms.

Proof. We start by expressing the sum over $r^m(n)$ as an integral in terms of $F(s)$,

$$\sum_{n\le N} r^m(n) = \frac{1}{2\pi i}\int_{1+\eta-i\infty}^{1+\eta+i\infty} F(s)\frac{x^s}{s}\,\mathrm{d}s.$$

By Lemma 2.1, the error produced by truncating the integral at heights $\pm T$ is $E_1 + E_2$, where from (2.24),

$$E_1 = \frac{1}{T}\sum_{n<x} r^m(n)\left(\frac{x}{n}\right)^{1+\eta}\frac{1}{\log(x/n)},$$

and, from (2.19),

$$E_2 = \frac{1}{T}\sum_{n>x} r^m(n)\left(\frac{x}{n}\right)^{1+\eta}\frac{1}{\log(n/x)}.$$

We use $\eta = 2/\log x$ to give us $x^{1+\eta} = O(x)$ in our expressions for E_1 and E_2. Hardy and Wright (chapter 18, [11]) showed that for each $\delta > 0$, there exists a constant $A(\delta)$ such that $r(n) \leq A(\delta)n^{\delta}$. For fixed m, we let $\delta = \epsilon/m$ for $\epsilon > 0$ so that $r^m(n) = O(n^{\epsilon})$. We then divide each of the errors E_1 and E_2 into two parts, so that $E_1 = E_{11} + E_{12}$, where

$$E_{11} = O\left(\frac{1}{T}\sum_{n<x/2}\frac{x}{n^{1+\eta-\epsilon}}\frac{1}{\log(x/n)}\right),$$
$$E_{12} = O\left(\frac{1}{T}\sum_{x/2<n<x}\frac{x}{n^{1+\eta-\epsilon}}\frac{1}{\log(x/n)}\right),$$

and $E_2 = E_{21} + E_{22}$, where

$$E_{21} = O\left(\frac{1}{T}\sum_{x<n<3x/2} r^m(n)\frac{x}{n^{1+\eta-\epsilon}}\frac{1}{\log(n/x)}\right),$$
$$E_{22} = O\left(\frac{1}{T}\sum_{n>3x/2} r^m(n)\frac{x}{n^{1+\eta-\epsilon}}\frac{1}{\log(n/x)}\right).$$

We consider E_{11} where $x/n > 2$, so that $\log(x/n) > \log 2 > 2/3$, which gives $1/\log(x/n) < 3/2$. Then we consider the sum

$$\sum_{n<x/2}\frac{1}{n^{1+\eta-\epsilon}} < \int_0^{x/2}\frac{1}{y^{1+\eta-\epsilon}}\,\mathrm{d}y < \frac{x^{\epsilon}}{(\eta-\epsilon)x^{\eta}} < x^{\epsilon},$$

which gives us the order of magnitude term

$$E_{11} = O\left(\frac{x^{1+\epsilon}}{T}\right). \tag{2.22}$$

For E_{12}, we have $x/n < 2$, so that

$$\frac{x}{n^{1+\eta-\epsilon}} < 2\frac{1}{n^{\eta-\epsilon}} = O(x^{\epsilon}).$$

Hence

$$E_{12} = O\left(\frac{x^\epsilon}{T} \sum_{x/2<n<x} \frac{1}{\log(x/n)}\right).$$

We estimate the $1/\log(x/n)$ factor by using the identity $n \equiv x(1-u)$, to get

$$\log\left(\frac{x}{n}\right) = \log\left(\frac{1}{1-u}\right) = u + \frac{u^2}{2} + \cdots > u,$$

which means $1/\log(x/n) < 1/u = x/(x-n)$.

We sum $x/(x-n)$ over $x/2 < n < x$. For some positive integer v, with $N - v + 1 \leq n \leq N$, we consider the sequence of possible values of $x/(x-n)$,

$$2x, \frac{2x}{3}, \frac{2x}{5}, \ldots, \frac{2x}{2v-1}. \tag{2.23}$$

We now sum the sequence of possible values of $x/(x-n)$ given in (2.23) over values of v between 1 and V, so that $2V - 1 \leq x < 2V + 1$. The sum of the sequence of possible values of $x/(x-n)$ is less than or equal to $2x(\log(x)+1)$, so that

$$\sum_{x/2<n<x} \frac{1}{\log(x/n)} < 2x(\log(x) + 1),$$

and hence

$$E_{12} = O\left(\frac{x^{1+\epsilon} \log x}{T}\right). \tag{2.24}$$

We combine our results for E_{11} in (2.22) and E_{12} in (2.24) to get

$$E_1 = E_{11} + E_{12} = O\left(\frac{x^{1+\epsilon}}{T}\right) + O\left(\frac{x^{1+\epsilon} \log x}{T}\right) = O\left(\frac{x^{1+\epsilon} \log x}{T}\right). \tag{2.25}$$

Similarly for E_{21}, we have $x < n < 3x/2$, so that $x/n < 1$, and

$$\frac{x}{n^{1+\eta-\epsilon}} < \frac{1}{n^{\eta-\epsilon}} = O(x^\epsilon).$$

We estimate the $1/\log(n/x)$ term of E_{21} by setting $\mu = (n-x)/x$, so that $\log(n/x) = \log(1+\mu)$. We have, for the set of values of μ given by $x/n < 1$,

$$\log(1+\mu) = \mu - \frac{1}{2}\mu^2 + \frac{1}{3}\mu^3 - \ldots \geq \frac{3\mu}{4}. \tag{2.26}$$

Let $n = N + r$, with n, N and r all positive integers. Since $x = N + 1/2$ is stated in the Lemma, we can express μ in terms of r and x, $\mu = (2r-1)/2x$.

We substitute this for μ in the inequality of (2.26), hence

$$\frac{1}{\log(n/x)} \leq \frac{8x}{3(2r-1)}.$$

We estimate the sum over the $1/\log(n/x)$ term by replacing the range of summation $x < n < 3x/2$ with $1/2 < r < N/2 + 3/4$, using $n = N + r$ and $x = N + 1/2$. Since r is an integer our values of r are between 1 and $N/2$, for N even, and our values of r are between 1 and $N/2 + 1/2$ for N odd. We need

$$\sum_{1/2<r<N/2+3/4} \frac{1}{2r-1} = \begin{cases} 1 + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{N-1} & N \text{ even}, \\ 1 + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{N} & N \text{ odd}. \end{cases}$$

This sum will be less than $\log x + 1$, regardless of whether N is even or odd. Hence

$$\sum_{x<n<3x/2} \frac{1}{\log(n/x)} \leq \frac{8x}{3} \sum_{x<n<3x/2} \frac{1}{2r-1} \leq \frac{8x}{3}(\log x + 1),$$

and

$$E_{21} = O\left(\frac{x^{1+\epsilon}\log x}{T}\right). \tag{2.27}$$

We now consider E_{22} with $n > 3x/2$. We find $\log(n/x) > \log(3/2) > 2/5$, so that $1/\log(n/x) < 5/2$. We estimate

$$\sum_{n>3x/2} \frac{1}{n^{1+\eta-\epsilon}} < \int_{3x/2-1}^{\infty} \frac{1}{y^{1+\eta-\epsilon}}\,\mathrm{d}y < \frac{1}{(\eta-\epsilon)x^{\eta-\epsilon}} < x^{\epsilon},$$

and therefore obtain

$$E_{22} = O\left(\frac{x^{1+\epsilon}}{T}\right). \tag{2.28}$$

We now use the results for E_{21} in (2.27) and E_{22} in (2.28) to express E_2 as an order of magnitude term,

$$E_2 = E_{21} + E_{22} = O\left(\frac{x^{1+\epsilon}\log x}{T}\right) + O\left(\frac{x^{1+\epsilon}}{T}\right) = O\left(\frac{x^{1+\epsilon}\log x}{T}\right). \tag{2.29}$$

Thus, overall, if we truncate at $1 + \eta \pm iT$, we do so with the error $E_1 + E_2$, which from the results of (2.25) and (2.29) gives us the order of magnitude

term

$$O\left(\frac{x^{1+\epsilon}\log x}{T}\right), \tag{2.30}$$

and Lemma 2.2 is proved. □

2.5 An estimate for the contour integral and calculation of the residue

We use Huxley's upper bound for the zeta function, given in [18], which takes the form

$$\zeta\left(\frac{1}{2}+it\right) \ll T^{\phi}(\log T)^{\gamma},$$

with $\phi = 32/205$ and $\gamma = 4157/2050$, and we estimate the contour integral.

Lemma 2.3. *In Lemma 2.2, we can choose $T \geq 10$ so that, for large x,*

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(s)\frac{x^s}{s}\,\mathrm{d}s = \operatorname*{Res}_{s=1} F(s)\frac{x^s}{s} + O\left(x^{\Phi+\epsilon}\right), \tag{2.31}$$

where $T = x^{1-\Phi}$, in the notation (2.2) *for Φ, and we use our convention on exponents ϵ.*

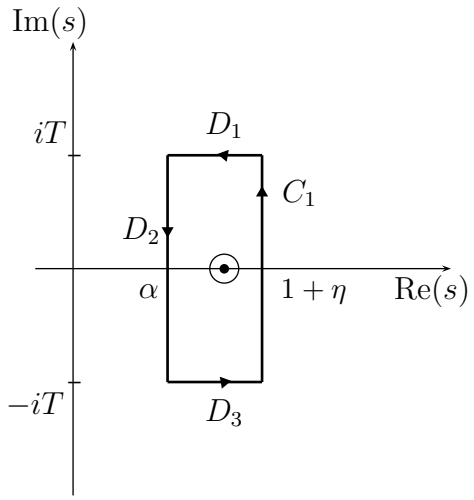
Proof. Cauchy's Residue Theorem states that

$$\frac{1}{2\pi i}\oint_D F(s)\frac{x^s}{s}\,\mathrm{d}s = \operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right],$$

where D is a bounded closed contour, depicted in Figure 2.3, and $s = 1$ is the pole of the integrand. Let $\alpha = 1/2 + 1/\log x$. Let $T \geq 10$ be a parameter; T will be chosen in such a way that T will be a fractional power of x. The contour $D = C_1 + D_1 + D_2 + D_3$ is constructed once a second parameter U in $T/2 \leq U \leq T$ has been chosen. Then C_1 is the line segment from $1+\eta+iU$ to $1+\eta-iU$, D_1 is the line segment from $1+\eta+iU$ to $\alpha+iU$, D_2 is the line segment from $\alpha+iU$ to $\alpha-iU$, and D_3 is the line segment from $\alpha-iU$ to $1+\eta-iU$.

Therefore, using Cauchy's Residue Theorem on the closed contour D, the

Figure 2.3: Contour D



integral along C_1 is

$$\frac{1}{2\pi i}\int_{C_1} F(s)\frac{x^s}{s}\,\mathrm{d}s = \operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right] - \frac{1}{2\pi i}\int_{D_1} F(s)\frac{x^s}{s}\,\mathrm{d}s - \frac{1}{2\pi i}\int_{D_2} F(s)\frac{x^s}{s}\,\mathrm{d}s - \frac{1}{2\pi i}\int_{D_3} F(s)\frac{x^s}{s}\,\mathrm{d}s. \tag{2.32}$$

To estimate the integrals along the contours D_1, D_2, and D_3, we use the identity $F(s) = Z^{b+1}(s)E(s)$. Firstly we consider the integral along D_2.

Along D_2 we have $\sigma = \alpha$ so that $E(s) \leq \tilde{J}\zeta^d(2\alpha)$. Now $2\alpha = 1 + 2/\log x$, and $\zeta(1+\delta) \leq 1 + 1/\delta$, which means that $\zeta(2\alpha) \leq 1 + (\log x)/2 \leq \log x$, provided that $x \geq e^2$, where here e is Napier's constant. Hence for $x \geq e^2$, we have $E(s) \leq \tilde{J}(\log x)^d$.

For $1 \leq \tau \leq T$ and $1/2 \leq \alpha \leq 3/4$,

$$\int_1^\tau |\zeta(\alpha + it)|^4\,\mathrm{d}t \ll \tau(\log\tau)^4 \ll T(\log T)^4, \tag{2.33}$$

[Titchmarsh, [37] chapter 7], so that

$$\int_{-T}^{T} \frac{|\zeta(\alpha+it)|^4}{|\alpha+it|}\,\mathrm{d}t \ll (\log T)^5. \tag{2.34}$$

The proof in [18] of Huxley's estimate

$$\zeta\left(\frac{1}{2}+it\right) \ll t^{\phi}(\log t)^{\gamma},$$

with $\phi = 32/205$ and $\gamma = 4157/2050$ and $10 \le |t| \le T$ can be adapted by standard methods [Huxley [15], Huxley and Watt [21]] to show that for $\sigma \ge 1/2$, $10 \le |t| \le T$,

$$\zeta(\sigma+it) \ll |t|^{2\phi(1-\sigma)}(\log|t|)^{\gamma} \ll T^{2\phi(1-\sigma)}(\log T)^{\gamma} \ll T^{\phi}(\log T)^{\gamma}, \quad (2.35)$$

and

$$L(\sigma+it,\chi) \ll |t|^{2\phi(1-\sigma)}(\log|t|)^{\gamma} \ll T^{2\phi(1-\sigma)}(\log T)^{\gamma} \ll T^{\phi}(\log T)^{\gamma}. \quad (2.36)$$

We use (2.35) and (2.36) to obtain

$$\int_{-T}^{T} \frac{|\zeta(\alpha+it)|^{b+1}|L(\alpha+it,\chi)|^{b+1}}{|\alpha+it|}\,\mathrm{d}t \ll (\log T)^5(T^{\phi}(\log T)^{\gamma})^{2(b-1)}. \quad (2.37)$$

Hence,

$$\begin{aligned}\int_{D_2} \frac{|F(s)|\,|x|^s}{|s|}|\,\mathrm{d}s| &\ll \int_{-T}^{T} |x^s|\,|E(s)|\frac{|\zeta(s)|^{b+1}|L(s,\chi)|^{b+1}}{|s|}\,\mathrm{d}t \\ &\ll \left(T^{2\phi(1-\alpha)}(\log T)^{\gamma}\right)^{2b-2} x^{\alpha}(\log x)^d \int_{-T}^{T} \frac{|\zeta(\alpha+it)|^4}{|\alpha+it|}\,\mathrm{d}t \\ &\ll \sqrt{x}T^{(2b-2)\phi}(\log T)^{(2b-2)\gamma+5}(\log x)^d, \end{aligned} \quad (2.38)$$

using $|E(s)| \ll (\log x)^d$ and $x^{\alpha} = ex^{1/2}$.

We now estimate the integrals along D_1 and D_3. Along D_1 and D_3 we have $\alpha \le \sigma \le 1+\eta$, $|x^s| = x^{\sigma}$, and

$$|E(s)| \le \tilde{J}\zeta^d(2\sigma) \ll \frac{1}{(2\sigma-1)^d} \ll \frac{1}{(2\alpha-1)^d} \ll (\log x)^d.$$

The integral along D_1 is found by averaging over U, $T/2 \le U \le T$,

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{D_1} F(s)\frac{x^s}{s}\,\mathrm{d}s\right| &\le \frac{1}{T/2}\int_{T/2}^{T}\int_{\alpha}^{1+\eta} \frac{|F(s)|\,|x^s|}{|s|}|\,\mathrm{d}s|\,\mathrm{d}t \\ &= \frac{2}{T}\int_{\alpha}^{1+\eta} x^{\sigma}\left(\int_{T/2}^{T}\frac{|Z^{b+1}(s)E(s)|}{|s|}\,\mathrm{d}t\right)\mathrm{d}\sigma. \end{aligned} \quad (2.39)$$

We use the bounds of equations (2.33), (2.35) and (2.36) to estimate

$$\begin{aligned}
&\int_{T/2}^{T} \frac{|Z^{b+1}(s)E(s)|}{|s|}\,\mathrm{d}t \\
&\ll (\log x)^d \int_{T/2}^{T} \frac{|\zeta(\sigma+it)|^{b+1}|L(\sigma+it,\chi)|^{b+1}}{|\sigma+it|}\,\mathrm{d}t \\
&\ll \frac{(\log x)^d\ T(\log T)^4\left(\max\{|\zeta(\sigma+it)|\}\right)^{b-3}\left(\max\{|L(\sigma+it,\chi)|\}\right)^{b+1}}{\min\{|\sigma+it|\}} \\
&\ll \frac{(\log x)^d\ T(\log T)^4\left(T^{2\phi(1-\sigma)}(\log T)^{\gamma}\right)^{b-3}\left(T^{2\phi(1-\sigma)}(\log T)^{\gamma}\right)^{b+1}}{T/2} \\
&\ll (\log x)^d\ T^{2\phi(1-\sigma)(2b-2)}(\log T)^{\gamma(2b-2)+4}. \qquad (2.40)
\end{aligned}$$

We substitute (2.40) into (2.39) to obtain

$$\begin{aligned}
\left|\frac{1}{2\pi i}\int_{D_1} F(s)\frac{x^s}{s}\,\mathrm{d}s\right| &\ll \frac{(\log x)^d(\log T)^{\gamma(2b-2)+4}}{T}\int_{\alpha}^{1+\eta} x^{\sigma}T^{2\phi(1-\sigma)(2b-2)}\,\mathrm{d}\sigma \\
&\ll \frac{(\log x)^d(\log T)^{\gamma(2b-2)+4}}{T}\max_{\alpha\le\sigma\le 1+\eta}\left\{x^{\sigma}T^{2\phi(1-\sigma)(2b-2)}\right\} \\
&\ll \frac{(\log x)^d(\log T)^{\gamma(2b-2)+4}}{T}\left(\sqrt{x}T^{(2b-2)\phi}+x\right). \qquad (2.41)
\end{aligned}$$

We get the same estimate for the integral along D_3.

We choose T so that $T^{(4b-4)\phi} \ll x$, which gives $\log T \ll \log x$. We can now modify the estimate (2.41) to be

$$\frac{1}{2\pi i}\int_{D_1} F(s)\frac{x^s}{s}\,\mathrm{d}s \ll \frac{x(\log x)^{(2b-2)\gamma+d+4}}{T},$$

and similarly we modify the estimate (2.38) for the integral along D_3. The estimate becomes

$$\frac{1}{2\pi i}\int_{D_2} F(s)\frac{x^s}{s}\,\mathrm{d}s \ll \sqrt{x}T^{(2b-2)\phi}(\log x)^{(2b-2)\gamma+d+5}.$$

We need to choose T to balance the terms found by estimating the integrals along D_1, D_2 and D_3, that is, we need to choose T such that

$$\frac{x(\log x)^{(2b-2)\gamma+d}+4}{T} \asymp x^{1/2}(\log x)^{(2b-2)\gamma+d+5}T^{(2b-2)\phi}.$$

Rearranging, we see that we have chosen T so that

$$T \asymp x^{1/((4b-4)\phi+2)} (\log x)^{-((2b-2)\phi+1)}. \tag{2.42}$$

Thus

$$\sqrt{x}T^{(2b-2)\phi}(\log x)^{(2b-2)\gamma+d+5} \asymp \frac{x(\log x)^{(2b-2)\gamma+d+4}}{T} \asymp x^{\Phi}(\log x)^{A},$$

with Φ as in (2.2), and $A = (2b-2)\gamma + d + 4$. The powers of $\log x$ contribute to the factor of the form x^{ϵ}. □

We now calculate the residue given in our contour integral estimation.

Lemma 2.4. *The residue in the statement of Lemma 2.3 can be written as*

$$\operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right] = xP_m(\log x),$$

where $P_m(z)$ is a polynomial in z of degree $b = 2^{m-1} - 1$.

Proof. The function $F(s)$ can be written as $Z^{b+1}(s)E(s)$, where $Z(s)$ is the Dedekind zeta function with a simple pole at $s = 1$, and $E(s)$ is the Euler product of (2.8), regular at $s = 1$. We express the coefficients of the polynomial $P_m(z)$ in terms of the derivatives of the function

$$V(s) = \frac{(s-1)^{b+1}F(s)}{s}, \tag{2.43}$$

which is regular at $s = 1$. Hence $V(s)$ is analytic and single-valued at $s = 1$, so $V(s)$ can be expanded as a power series on a neighbourhood of $s = 1$,

$$V(s) = \sum_{n=0}^{\infty} \frac{V^{(n)}(1)}{n!}(s-1)^n.$$

From (2.43) we can express

$$F(s)\frac{x^s}{s} = \frac{V(s)x^s}{(s-1)^{b+1}},$$

and we use this to write the residue as a limit,

$$\operatorname*{Res}_{s=1}\left[F(s)\frac{x^s}{s}\right] = \operatorname*{Res}_{s=1}\left[\frac{V(s)x^s}{(s-1)^{b+1}}\right] = \lim_{s\to 1}\left[\frac{1}{b!}\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^b V(s)\frac{x^s}{s}\right].$$

The result of the Lemma follows by the usual rules of differentiation, since

$$\lim_{s\to 1}\left[\frac{1}{b!}\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^b V(s)\frac{x^s}{s}\right] = \frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(1)x(\log x)^j,$$

where $V^{(b-j)}(s)$ denotes the $(b-j)$th derivative of $V(s)$ with respect to s, and $V^{(0)}(s) = V(s)$, and we write

$$P_m(z) = \frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(1)z^j.$$

□

2.6 Remainder of the proof of Theorem 1

Concatenating the results of Lemmas 2.2, 2.3, and 2.4, we have

$$\sum_{n\le N} r^m(n) = xP_m(\log x) + O\left(x^{\Phi+\epsilon}\right) + O\left(\frac{x^{1+\epsilon}\log x}{T}\right). \tag{2.44}$$

By the choice of T in Lemma 2.3 the error terms combine in the form $O\left(x^{\Phi+\epsilon}\right)$ under our convention on exponents ϵ. The result of Theorem 1 is expressed in terms of $N = x - 1/2$, so that

$$x = N\left(1 + O\left(\frac{1}{N}\right)\right), \quad \log x = \log N + O\left(\frac{1}{N}\right),$$

and we pass easily from the expression (2.44) in terms of x to the statement (2.1) of Theorem 1 in terms of N. □

2.7 The leading coefficient of the polynomial $P_m(x)$

The leading coefficient c of the polynomial $P_m(x)$ of Theorem 1 is $V(1)/b!$. Since $V(s)$ is regular at $s = 1$ we know it takes a single value at $s = 1$. We have

$$V(1) = \frac{E(1)}{1}\left(\lim_{s\to 1}(s-1)Z(s)\right)^{b+1},$$

and as s tends to 1, $(s-1)Z(s) = (s-1)\zeta(s)L(s,\chi)$ tends to $L(1,\chi) = \pi/4$. Thus the leading coefficient of $P_m(x)$ is

$$c = \left(\frac{\pi}{4}\right)^{b+1} \frac{E}{b!}; \tag{2.45}$$

where E is the Euler product

$$E = \left(\frac{1}{2}\right)^{b} \prod_{p\equiv 1 \bmod 4} \left(1-\frac{1}{p}\right)^{A(m,2)} \sum_{k=1}^{m} A(m,k)p^{(1-k)} \prod_{p\equiv 3 \bmod 4} \left(1-\frac{1}{p^2}\right)^{b}, \tag{2.46}$$

and $A(m,k)$ denotes the Eulerian number [2],

$$A(m,k) = \sum_{j=0}^{k} (-1)^j \, {}_{m+1}\mathrm{C}_j (k-j)^m, \tag{2.47}$$

with $A(m,2) = 2^m - m - 1$. We find $E = E(1)$ given in (2.46) from (2.8) with $s = 1$.

2.8 Asymptotic formulae for the number of cyclic polygons with m integer vertices

We can now establish asymptotic formulae for the number of cyclic polygons with m integer vertices, for each $m \geq 3$, which have circumcentre at the origin and circumradius at most $\sqrt{N}$ as a direct result of our work in Theorem 1.

Theorem 2. *Let $m \geq 3$ be a fixed integer. Let $X_m(N)$ denote the number of cyclic polygons with circumcentre at the origin, m integer vertices, and circumradius at most $\sqrt{N}$. Then*

$$X_m(N) = \frac{N}{m!} \left(\sum_{j=1}^{m} 4^j s(m,j) P_j(\log N) \right) + O\left(N^{\Phi+\epsilon}\right).$$

The polynomials $P_j(x)$ and the exponent Φ are as in Theorem 1, where b in (2.2) is the degree of $P_m(x)$.

Proof. We recall that $X_m(N)$ denotes the number of cyclic polygons with m integer vertices, centre at the origin, and circumradius at most $\sqrt{N}$. The radius squared is an integer n. Let $Y_m(n)$ be the number of such polygons

inscribed in the circle $x^2 + y^2 = n$. Then $Y_m(n) = {}_rC_m$, where $r = 4r(n)$ and $Y_m(n)$ can be expanded in terms of $s(m, j)$, the signed Stirling numbers of the first kind [4], to give

$$Y_m(n) = \frac{1}{m!} \sum_{j=1}^{m} s(m, j) \, (4r(n))^j \, .$$

Hence

$$\begin{aligned} X_m(N) &= \sum_{n \le N} Y_m(n) \\ &= \sum_{n \le N} \frac{1}{m!} \sum_{j=1}^{m} s(m, j) \, (4r(n))^j \\ &= \frac{1}{m!} \sum_{j=1}^{m} 4^j s(m, j) \sum_{n \le N} r^j(n). \end{aligned} \tag{2.48}$$

Theorem 2 follows at once when we substitute the asymptotic expansion (2.1) of Theorem 1. The error exponent Φ in (2.2) is a function of $b = 2^{j-1} - 1$ in our present notation, and has its largest value when $j = m$, so the error exponent Φ in (2.48) is formally the same as that of (2.2) with $b = 2^{m-1} - 1$. □

Chapter 3

Results for the function $r^*(n,q)$

3.1 Lemmas involving the function $r^*(n,q)$

We now consider an arithmetic function $r^*(n,q)$ related to the arithmetic function $r(n)$. Let q be a fixed positive integer, then $r^*(n,q)$ is the arithmetic function which counts the integer solutions of $x^2+y^2=n$ with $x>0$, $y\geq 0$ and highest common factor $(x,y,q)=1$. The aim is to produce a Theorem for powers of $r^*(n,q)$ analogous to Theorem 1. Before we can do this, we need to know more about the properties of $r^*(n,q)$. We express the properties of $r^*(n,q)$ that we need in the form of several lemmas.

Lemma 3.1. *The arithmetic function $r^*(n,q)$ can be written in terms of $r(n)$, the number of integer solutions of $x^2+y^2=n$ with $x>0$ and $y\geq 0$, and $\mu(d)$, the Möbius function, as follows:*

$$r^*(n,q)=\sum_{\substack{d|q\\ d^2|n}}\mu(d)r\left(\frac{n}{d^2}\right). \tag{3.1}$$

Proof. From the definition of $r^*(n,q)$ as the number of integer solutions of $x^2+y^2=n$ with $x>0$, $y\geq 0$, and $(x,y,q)=1$, we can express $r^*(n,q)$ in terms of the Möbius function $\mu(d)$,

$$r^*(n,q)=\sum_{\substack{x>0\\ x^2+y^2=n}}\sum_{\substack{y\geq 0\\ d|x\\ d|y\\ d|q}}\sum\mu(d).$$

Let $x = ds$ and $y = dt$ with $d > 0$, $s > 0$ and $t \geq 0$ then this becomes

$$r^*(n,q) = \sum_{\substack{ds>0 \\ (ds)^2+(dt)^2=n}} \sum_{dt\geq 0} \sum_{\substack{d|q \\ d^2|n}} \mu(d),$$

which rearranges to give

$$r^*(n,q) = \sum_{\substack{d|q \\ d^2|n}} \mu(d) \sum_{\substack{s \\ s^2+t^2=\frac{n}{d^2}}} \sum_{t} 1 = \sum_{\substack{d|q \\ d^2|n}} \mu(d) r\left(\frac{n}{d^2}\right).$$

□

We now show that $r^*(n,q)$ is a multiplicative function, although $r^*(n,q)$ is not completely multiplicative. A function f is multiplicative if, when $(m,n) = 1$, we have $f(mn) = f(m)f(n)$. It is completely multiplicative if we can remove the coprimality condition $(m,n) = 1$.

Lemma 3.2. *For fixed q, $r^*(n,q)$ is a multiplicative function.*

Proof. We use the definition of $r^*(n,q)$ from Lemma 3.1. It is widely known that $\mu(n)$ is multiplicative, see chapter 4, Hardy and Wright [13], for a proof. We explained in the proof of Theorem 1 that $r(n)$ is multiplicative.

Let $(m,n) = 1$, then we show that $r^*(mn,q) = r^*(m,q)r^*(n,q)$. By the definition in (3.1),

$$r^*(mn,q) = \sum_{\substack{d|q \\ d^2|mn}} \mu(d) r\left(\frac{mn}{d^2}\right).$$

Let $d = ab$ with $(a,b) = 1$, then since $d|q$, it is clear that $a|q$ and $b|q$. As $d^2|mn$ means that $(ab)^2|mn$, we can choose a and b in such a way that $a^2|m$ and $b^2|n$ since both of the highest common factors (a,b) and (m,n) are equal to 1. If $d^2|m$, then $d^2 = a^2$ and $b = 1$, and similarly if $d^2|n$, then $d^2 = b^2$ and $a = 1$. Hence

$$r^*(mn,q) = \sum_{\substack{ab|q \\ (ab)^2|mn}} \mu(ab) r\left(\frac{mn}{a^2b^2}\right) = \sum_{\substack{a|q \\ a^2|m}} \sum_{\substack{b|q \\ b^2|m}} \mu(a)\mu(b) r\left(\frac{m}{a^2}\right) r\left(\frac{n}{b^2}\right), \quad (3.2)$$

using the multiplicativity of $\mu(d)$ and $r(n)$. We rearrange (3.2) to obtain

$$r^*(mn,q) = \sum_{\substack{a|q \\ a^2|m}} \mu(a) r\left(\frac{m}{a^2}\right) \sum_{\substack{b|q \\ b^2|n}} \mu(b) r\left(\frac{n}{b^2}\right) = r^*(m,q) r^*(n,q).$$

Hence $r^*(n,q)$ is multiplicative. □

We find expressions for $r^*(n,q)$ related to the primes p, which will allow us to calculate the value of $r^*(n,q)$ for any integer n, because of the multiplicative property of $r^*(n,q)$. We distinguish between the primes p which divide q and the primes p which do not divide q. We call a prime p good if $p \nmid q$, and we call a prime p bad if $p \mid q$.

Lemma 3.3. *Let $n = p^k$, where $p \geq 2$ is a prime, and $k \geq 1$ is an integer. Then*

$$r^*(n,q) = \begin{cases} r(n) & \text{for all primes when } k = 1, \\ r(n) & \text{for good primes } p, \text{ when } k \geq 2, \\ 0 & \text{for } p = 2 \text{ bad, when } k \geq 2, \\ 2 & \text{for bad } p \equiv 1 \bmod 4, \\ 0 & \text{for bad } p \equiv 3 \bmod 4. \end{cases}$$

Proof. When $k = 1$ we have $r^*(n,q) = r^*(p,q)$ which we express in terms of $r(n)$ and $\mu(d)$,

$$r^*(p,q) = \sum_{\substack{d|q \\ d^2|p}} \mu(d) r\left(\frac{p}{d^2}\right) = \mu(1) r\left(\frac{p}{1^2}\right) = r(p).$$

This is since the only divisor d of a prime p which satisfies $d^2|p$ is $d = 1$.

Using $n = p^k$ gives us $r^*(n,q) = r^*(p^k,q)$, where

$$r^*(p^k,q) = \sum_{\substack{d|q \\ d^2|p^k}} \mu(d) r\left(\frac{p^k}{d^2}\right).$$

When $d^2|p^k$ then d is potentially equal to $1, p, p^2, \ldots$, and $d \leq p^{k/2}$. However $d|q$ as well, and since p is good, $p \nmid q$, the only possible divisor d satisfying $d|q$, $p \nmid q$ and $d^2|p^k$ is $d = 1$, so that $r^*(p^k,q) = r(p^k)$. If p is bad then

$p \mid q$, and the only divisors d of p^k that we need to consider are those divisors which are square-free, since if d is not square-free, $\mu(d) = 0$. Hence we only consider $d = 1$ and $d = p$. We have $k \geq 2$, so that $r^*(n, q) = r^*(p^k, q) = r(p^k) - r(p^{k-2})$. For $p = 2$, this equals 0. For $p \equiv 1 \bmod 4$, $r(p^k) = k + 1$ and $r(p^{k-2}) = k - 1$ so $r^*(p^k, q)$ equals 2.

We consider $p \equiv 3 \bmod 4$ separately. A prime $p \equiv 3 \bmod 4$ can only be expressed as the sum of two squares when it is taken to an even power. Thus $n = p^{2k}$, satisfying $x^2 + y^2 = p^{2k}$. The solutions of this equation are either $x = p^k$ and $y = 0$, or $x = 0$ and $y = p^k$. Neither of these solutions will give $(x, y, q) = 1$, so they do not count towards the quantity $r^*(n, q)$ and thus $r^*(p^k, q) = 0$ when $p \equiv 3 \bmod 4$. □

3.2 Theorem 3 on sums of m-th powers of the function $r^*(n, q)$

Theorem 3. *Let $m \geq 3$ and $q \geq 1$ be fixed integers. Let $r^*(n, q)$ be the arithmetic function which counts integer solutions of $x^2 + y^2 = n$ with $x > 0$, $y \geq 0$ and highest common factor $(x, y, q) = 1$, then for $\mathrm{Re}(s) = \sigma > 1/2$, as $N \to \infty$,*

$$\sum_{n \leq N} \frac{(r^*(n, q))^m}{n^s} = N \ P_{m,q}(\log N) + O(q^\epsilon N^{\Phi + \epsilon}), \tag{3.3}$$

where $P_{m,q}(z)$ is a polynomial of degree $b = 2^{m-1} - 1$ whose coefficients depend on q, and $\Phi < 1$ is the same exponent as in (2.2) of Theorem 1. The leading coefficient c_q of $P_{m,q}(x)$ can be expressed as

$$c_q = \frac{1}{b!} \left(\frac{\pi}{4}\right)^{b+1} E(q, 1), \tag{3.4}$$

where $E(q, 1) = E\Psi(q, 1)$, for E as in (2.46) of Theorem 1, and $\Psi(q, 1)$ is a certain convergent Euler product defined in (3.14) below.

3.3 Proof of Theorem 3

We write the Dirichlet series $F(q, s)$ for $(r^*(n, q))^m$ as an Euler product

$$F(q, s) = \sum_{n=1}^{\infty} \frac{(r^*(n, q))^m}{n^s} = \prod_{p \text{ prime}} \phi_p(q, s).$$

For good primes $p \nmid q$ the Euler factors are those in (2.5),

$$\phi_p(q,s) = \phi_p(s) = \begin{cases} G\left(\dfrac{1}{2^s}\right) & \text{for } p = 2, \\ H\left(\dfrac{1}{p^s}\right) & \text{for } p \equiv 1 \bmod 4, \\ G\left(\dfrac{1}{p^{2s}}\right) & \text{for } p \equiv 3 \bmod 4. \end{cases}$$

For bad primes $p \mid q$ the Euler factors become

$$\phi_p(q,s) = \theta_p(s) = \begin{cases} 1 + \dfrac{1}{2^s} & \text{for } p = 2, \\ 1 + \dfrac{2^m}{p^s - 1} & \text{for } p \equiv 1 \bmod 4, \\ 1 & \text{for } p \equiv 3 \bmod 4. \end{cases}$$

We want a factorisation

$$F(q,s) = Z^{b+1}(s)E(q,s) = Z^{b+1}(s)E(s)\Psi(q,s),$$

where $\Psi(q,s)$ is a finite Euler product,

$$\Psi(q,s) = \prod_{p|q} \psi_p(s), \tag{3.5}$$

and $\psi_p(s) = \theta_p(s)/\phi_p(s)$, so that

$$\psi_p(s) = \begin{cases} 1 - \dfrac{1}{p^{2s}} & \text{for } p \not\equiv 1 \bmod 4, \\ \dfrac{1 + 2^m/(p^s - 1)}{H\left(1/p^s\right)} & \text{for } p \equiv 1 \bmod 4. \end{cases} \tag{3.6}$$

The most difficult case we consider is when $p \equiv 1 \bmod 4$. Instead of the Euler factor at good primes

$$H\left(\frac{1}{p^s}\right) = 1 + \frac{2^m}{p^s} + \frac{3^m}{p^{2s}} + \frac{4^m}{p^{3s}} + \dots \ ,$$

we have

$$1 + \frac{2^m}{p^s - 1} = 1 + \frac{2^m}{p^s} + \frac{2^m}{p^{2s}} + \frac{2^m}{p^{3s}} + \dots \ .$$

Taking out the factor $Z^{b+1}(s) = (\zeta(s)L(s,\chi))^{b+1} = (\zeta(s)L(s,\chi))^{2^{m-1}}$ makes the Euler factor more complicated. At good primes the Euler factor becomes

$$\left(1-\frac{1}{p^s}\right)^{2^m}\left(1+\frac{2^m}{p^s}+\frac{3^m}{p^{2s}}+\frac{4^m}{p^{3s}}+\dots\right) = 1-\frac{d}{p^{2s}}+\frac{d_3}{p^{3s}}-\frac{d_4}{p^{4s}}+\dots\ , \quad (3.7)$$

where $d = 2^{m-1}(2^m+1)-3^m$ as in (2.10), $d_3 = 4^m - 6^m + (8^m - 2^m)/3$, and the coefficients d_4 onwards can be calculated.

At bad primes the Euler factor becomes

$$\left(1-\frac{1}{p^s}\right)^{2^m}\left(1+\frac{2^m}{p^s-1}\right) = 1-\frac{e_2}{p^{2s}}+\frac{e_3}{p^{3s}}+\dots-\frac{e_{2^m}}{p^{2^m s}}, \quad (3.8)$$

where $e_2 = 2^{m-1}(2^m-1)$, $e_3 = (8^m+2^{m+1})/3 - 4^m$, and the coefficients e_4 to e_{2^m} can be calculated.

We need to consider the convergence and the size of $E(q,s)$. The finite Euler product $\Psi(q,s)$ does not affect the convergence of the product $E(q,s) = E(s)\Psi(q,s)$, which is convergent for $\mathrm{Re}(s) \geq 1/2$, since $E(s)$ is convergent in this region, as are the expressions in (3.6), (3.7) and (3.8). Poles at points s where some factor $H(1/p^s)$ vanishes are removable in the product $E(s)\Psi(q,s)$.

With respect to the size of $E(q,s)$, we express this factor in a manner analogous to that of (2.9) as

$$E(q,s) = \frac{J(q,s)}{\zeta^{j_1}(2s)L^{j_2}(s,\chi)},$$

where $j_1 = (d+b)/2$ and $j_2 = (d-b)/2$.

We take out the correct Euler factor $(1-1/p^{2s})^d$ for the good primes $p \equiv 1 \bmod 4$. At bad primes $p \equiv 1 \bmod 4$ we have a partially cancelled Euler factor

$$\frac{1-\frac{e}{p^{2s}}+\frac{e_3}{p^{3s}}-\frac{e_4}{p^{4s}}+\dots}{\left(1-\frac{1}{p^{2s}}\right)^d}. \quad (3.9)$$

Our minimum value of σ is $1/2 + 1/\log x$, which gives $|p^{-2s}| \leq 1/p$. The

modulus of the expression in (3.9) is less than or equal to

$$\frac{1+\dfrac{e}{p}+\dfrac{e_3}{p^{3/2}}+\dots}{\left(1-\dfrac{1}{p}\right)^d} \le \frac{\left(1+\dfrac{1}{\sqrt{p}}\right)^{2^m}\left(1+\dfrac{2^m}{\sqrt{p}-1}\right)}{\left(1-\dfrac{1}{p}\right)^d},$$

when $\sigma \ge 1/2$.

To estimate this we split the primes $p|q$, $p \equiv 1 \bmod 4$, into two ranges, $p < (2^m+1)^2$ and $p \ge (2^m+1)^2$. We have

$$1+\frac{2^m}{\sqrt{p}-1} \le \begin{cases} 2 & \text{for } p \ge (2^m+1)^2, p \equiv 1 \bmod 4 \\ 2^m & \text{for } p < (2^m+1)^2, p \equiv 1 \bmod 4. \end{cases}$$

We know the size of $E(s)$, and since $E(q,s) = E(s)\Psi(q,s)$ we need only consider the product $\Psi(q,s)$ over bad primes in our size estimate.

We find

$$\begin{aligned} \prod_{\substack{p|q \\ p\equiv 1 \bmod 4}} \left(1+\frac{2^m}{\sqrt{p}-1}\right) &\le \prod_{\substack{p|q \\ p\equiv 1 \bmod 4 \\ p<(2^m+1)^2}} 2^m \prod_{\substack{p|q \\ p\equiv 1 \bmod 4 \\ p\ge(2^m+1)^2}} 2 \\ &\le (2^m)^{(2^{2m-1}+2^m)} d(q) \\ &= O(q^\epsilon). \end{aligned}$$

Also

$$\prod_{\substack{p|q \\ p\equiv 1 \bmod 4}} \frac{\left(1+\dfrac{1}{\sqrt{p}}\right)^{2^m}}{\left(1-\dfrac{1}{p}\right)^d} \le (B(\epsilon))^\omega q^\epsilon,$$

where ω is the number of distinct prime factors of q and $B(\epsilon)$ is a constant depending on ϵ. We use $B(\epsilon) = 2^{B_2(\epsilon)}$ and $2^{\omega(q)} \le d(q)$ to obtain

$$(B(\epsilon))^\omega q^\epsilon = \left(2^{B_2(\epsilon)}\right)^\omega q^\epsilon \le (d(q))^{B_2(\epsilon)} q^\epsilon = O(q^\epsilon),$$

following our conventions on exponents ϵ. Also we find the factor

$$\prod_{\substack{p|q \\ p\not\equiv 1 \bmod 4}} \left(1-\frac{1}{p^{2s}}\right) \le \prod_{\substack{p|q \\ p\not\equiv 1 \bmod 4}} \left(1-\frac{1}{p}\right) = O(q^\epsilon).$$

Thus the size of $E(q,s)$ is the size of $E(s)$ multiplied by the size of $\Psi(q,s)$ giving, for $\sigma \geq 1/2$,

$$E(q,s) \ll q^{\epsilon} \log^{d} x. \tag{3.10}$$

We now truncate our contour integrals. The standard method of truncating the contour integral which defines the Mellin transform for a single term of a Dirichlet series is given in Lemma 2.1 of Section 2.3. We use this to produce an analogous result to that of Lemma 2.2 by applying the truncation to the series $F(q,s)$ term-by-term, so that for N a positive integer, with $x = N + 1/2$ and $\eta = 2/\log x$, as $N \to \infty$,

$$\sum_{n \leq N} (r^*(n,q))^m = \frac{1}{2\pi i} \int_{1+\eta-iT}^{1+\eta+iT} F(q,s) \frac{x^s}{s} \, \mathrm{d}s + O\left(\frac{x^{1+\epsilon} \log x}{T} \right), \tag{3.11}$$

using our conventions on exponents ϵ, and remainder terms.

This result is proved similarly to Lemma 2.2. When we truncate at heights $\pm T$, we replace the errors E_1 and E_2 with the errors E_1^* and E_2^*, giving an overall error of $E_1^* + E_2^*$. We find E_1^* and E_2^* from the equations (2.16) and (2.21) of Lemma 2.1, with $\eta = 2/\log x$ and $x^{1+\eta} = O(x)$, so that we have

$$\begin{aligned} E_1^* =& O\left(\sum_{n<x} (r^*(n,q))^m \frac{x}{n^{1+\eta}} \frac{1}{T \log(x/n)} \right) \\ E_2^* =& O\left(\sum_{n>x} (r^*(n,q))^m \frac{x}{n^{1+\eta}} \frac{1}{T \log(n/x)} \right) \end{aligned}$$

By definition, $r^*(n,q)$ counts all integer solutions of $x^2 + y^2 = n$ for $x > 0$, $y \geq 0$ with $(x,y,q) = 1$, whereas $r(n)$ counts all integer solutions of $x^2 + y^2 = n$ for $x > 0$, $y \geq 0$. It is clear that therefore $r^*(n,q)$ is at most equal to $r(n)$ as it counts the size of a subset of the solutions to the equation $x^2 + y^2 = n$ for $x > 0$, $y \geq 0$. Thus, using the work of Hardy and Wright in chapter 19 of [13], there exists a constant $A(\delta)$ with $\delta > 0$, with $r^*(n,q) \leq r(n) \leq A(\delta) n^{\delta}$.

We now have the same situation as in Lemma 2.2, and we find the order of magnitude term

$$E_1^* + E_2^* = O\left(\frac{x^{1+\epsilon} \log x}{T} \right),$$

matching that of (2.30), and so we get the result of (3.11).

We estimate the contour integral in similar fashion to Lemma 2.3 in

Section 2.5.

Lemma 3.4. *In our result* (3.11)*, we choose* $T \geq 10$*, so that, for large* x*,*

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(q,s)\frac{x^s}{s}\,\mathrm{d}s = \operatorname*{Res}_{s=1}\left[F(q,s)\frac{x^s}{s}\right] + O\left(q^{\epsilon}x^{\Phi+\epsilon}\right), \tag{3.12}$$

where $T = x^{1-\Phi}$ *in the notation of* (2.2) *for* Φ*, and we observe our conventions on exponents* ϵ*.*

Proof. We use the contour D of Figure 2.3 with $\alpha = 1/2 + 1/\log(x)$. We want to find

$$\frac{1}{2\pi i}\int_{1+\eta-iT}^{1+\eta+iT} F(q,s)\frac{x^s}{s}\,\mathrm{d}s = \frac{1}{2\pi i}\int_{C_1} F(q,s)\frac{x^s}{s}\,\mathrm{d}s.$$

We change $F(s)$ to $F(q,s)$ in (2.32) to get

$$\begin{aligned}\frac{1}{2\pi i}\int_{C_1} F(q,s)\frac{x^s}{s}\,\mathrm{d}s = \operatorname*{Res}_{s=1}\left[F(q,s)\frac{x^s}{s}\right] - \frac{1}{2\pi i}\int_{D_1} F(q,s)\frac{x^s}{s}\,\mathrm{d}s \\ - \frac{1}{2\pi i}\int_{D_2} F(q,s)\frac{x^s}{s}\,\mathrm{d}s - \frac{1}{2\pi i}\int_{D_3} F(q,s)\frac{x^s}{s}\,\mathrm{d}s.\end{aligned}$$

We estimate the integrals along D_1, D_2, and D_3 by means of the identity $F(q,s) = Z^{b+1}(s)E(q,s)$, where $Z(s) = \zeta(s)L(s,\chi)$ is the Dedekind zeta function. We use also that $|E(q,s)| \ll q^{\epsilon}(\log x)^d$ as in (3.10), for $\sigma > 1/2$, where $d = 2^{m-1}(2^m+1) - 3^m$ as in (2.10).

We begin with the integral along D_2. We use the results of (2.37) and (2.38) to estimate

$$\begin{aligned}&\int_{-T}^{T} \frac{|x^s|\,|E(q,s)|}{|s|}|\zeta(s)|^{b+1}|L(s,\chi)|^{b+1}\,\mathrm{d}t \\ &\ll x^{\alpha}q^{\epsilon}(\log x)^d\left(T^{2\phi(1-\alpha)}(\log T)^{\gamma}\right)^{2b-2}\int_{-T}^{T}\frac{|\zeta(\alpha+it)|}{|\alpha+it|}\,\mathrm{d}t.\end{aligned}$$

Now $x^{\alpha} = ex^{1/2}$, which, along with the result of (2.34), enables us to conclude that the estimate of the integral along D_2 is

$$\left|\frac{1}{2\pi i}\int_{D_2} F(q,s)\frac{x^s}{s}\,\mathrm{d}s\right| \ll q^{\epsilon}\sqrt{x}T^{(2b-2)\phi}(\log T)^{(2b-2)\gamma+5}(\log x)^d.$$

We now estimate the integrals along D_1 and D_3. On D_1 and D_3 we have $\alpha \leq \sigma \leq 1+\eta$, $|x^s| = x^{\sigma}$, and $|E(q,s)| \leq q^{\epsilon}(\log x)^d$. We find the integral

along D_1 by averaging over U, $T/2 \le U \le T$, so that

$$\left|\frac{1}{2\pi i}\int_{D_1} F(q,s)\frac{x^s}{s}\,\mathrm{d}s\right| \le \frac{2}{T}\int_{\alpha}^{1+\eta} x^{\sigma}\left(\int_{T/2}^{T}\frac{|Z^{b+1}(s)E(q,s)|}{|s|}\,\mathrm{d}t\right)\,\mathrm{d}\sigma.$$

We adapt (2.40) to give

$$\int_{T/2}^{T}\frac{|Z^{b+1}(s)E(q,s)|}{|s|}\,\mathrm{d}t \ll q^{\epsilon}(\log x)^{d}T^{2\phi(1-\sigma)(2b-2)}(\log T)^{\gamma(2b-2)+4},$$

and we obtain, using the method of (2.41)

$$\left|\frac{1}{2\pi i}\int_{D_1} F(q,s)\frac{x^s}{s}\,\mathrm{d}s\right| \ll \frac{q^{\epsilon}(\log x)^{d}(\log T)^{\gamma(2b-2)+4}}{T}\left(\sqrt{x}T^{(2b-2)\phi}+x\right).$$

We get the same estimate for the integral along D_3.

We again choose $T \ge 10$ with $T^{(4b-4)\phi} \ll x$, and balance the terms found by estimating the integrals along D_1, D_2 and D_3 to get T as in (2.42),

$$T \asymp x^{1/((4b-4)\phi+2)}\left(\log x\right)^{-((2b-2)\phi+1)}.$$

Hence

$$q^{\epsilon}\sqrt{x}T^{(2b-2)\phi}(\log x)^{(2b-2)\gamma+d+5} \asymp \frac{q^{\epsilon}x(\log x)^{(2b-2)\gamma+d+4}}{T} \asymp q^{\epsilon}x^{\Phi}(\log x)^{A},$$

with Φ as in (2.2), and $A = (2b-2)\gamma + d + 4$. The powers of $\log x$ contribute to the factor of the form x^{ϵ}. □

We calculate the residue of (3.12) in the same way as we did for the residue in the proof of Theorem 1.

Lemma 3.5. *The residue of* (3.12) *can be written as*

$$\operatorname*{Res}_{s=1}\left[F(q,s)\frac{x^s}{s}\right] = xP_{m,q}(\log x),$$

where $P_{m,q}(z)$ is a polynomial in z of degree $b = 2^{m-1}-1$.

Proof. The function $F(q,s)$ can be written as $Z^{b+1}(s)E(q,s)$ where $Z(s)$ is the Dedekind zeta function with a simple pole at $s=1$, and $E(q,s)$ is an Euler product regular at $s=1$. We express the coefficients of the polynomial

$P_{m,q}(z)$ in terms of the derivatives of the function

$$V(q,s) = \frac{(s-1)^{b+1}F(q,s)}{s},$$

which is regular at $s = 1$. Hence $V(q,s)$ can be expanded as a power series on a neighbourhood of $s = 1$,

$$V(q,s) = \sum_{n=0}^{\infty} \frac{V^{(n)}(q,1)}{n!}(s-1)^n.$$

Then

$$\frac{F(q,s)x^s}{s} = \frac{V(q,s)x^s}{(s-1)^{b+1}},$$

and we use this to express the residue as a limit,

$$\operatorname*{Res}_{s=1}\left[F(q,s)\frac{x^s}{s}\right] = \operatorname*{Res}_{s=1}\left[\frac{V(q,s)x^s}{(s-1)^{b+1}}\right] = \lim_{s\to 1}\ \left[\frac{1}{b!}\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^b\ V(q,s)\frac{x^s}{s}\right].$$

The result of the Lemma follows by the usual rules of differentiation, since

$$\lim_{s\to 1}\ \left[\frac{1}{b!}\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^b\ V(q,s)\frac{x^s}{s}\right] = \frac{1}{b!}\sum_{j=0}^{b}\ {}_b\mathrm{C}_j V^{(b-j)}(q,1)x(\log x)^j,$$

where $V^{(b-j)}(q,s)$ denotes the $(b-j)$th derivative of $V(q,s)$ with respect to s, and $V^{(0)}(q,s) = V(q,s)$, and we write

$$P_{m,q}(z) = \frac{1}{b!}\sum_{j=0}^{b}\ {}_b\mathrm{C}_j V^{(b-j)}(q,1)z^j.$$

□

Concatenating the results of equations (3.11) and (3.12) we find

$$\sum_{n\le N}(r^*(n,q))^m = \operatorname*{Res}_{s=1}\Big[F(q,s)\frac{x^s}{s}\Big] + O\left(q^{\epsilon}x^{\Phi+\epsilon}\right) + O\left(\frac{x^{1+\epsilon}\log x}{T}\right). \quad (3.13)$$

By the choice of T in (2.42) the error terms combine in the form $O\left(q^{\epsilon}x^{\Phi+\epsilon}\right)$ under our convention on exponents ϵ. The result of Theorem 3 is expressed

in terms of $N = x - 1/2$, so that

$$x = N\left(1 + O\left(\frac{1}{N}\right)\right), \quad \log x = \log N + O\left(\frac{1}{N}\right),$$

and we pass easily from the expression (3.13) in terms of x to the statement (3.3) of Theorem 3 in terms of N.

The leading coefficient of $P_{m,q}(\log x)$ is $c_q = V(q,1)/b!$. We have

$$V(q,1) = \frac{E(q,1)}{1}\left(\lim_{s\to 1}(s-1)Z(s)\right)^{b+1},$$

and as s tends to 1, $(s-1)Z(s) = (s-1)\zeta(s)L(s,\chi)$ tends to $L(1,\chi) = \pi/4$. We therefore have

$$V(q,1) = E(q,1)\left(\frac{\pi}{4}\right)^{b+1},$$

and hence the leading coefficient c_q of $P_{m,q}(x)$ can be expressed as in (3.4) in the statement of the Theorem,

$$c_q = \frac{1}{b!}\left(\frac{\pi}{4}\right)^{b+1} E(q,1).$$

Thus we need to find an expression for $E(q,1)$. Since $E(q,s) = E(s)\Psi(q,s)$, we have $E(q,1) = E\Psi(q,1)$ for E is as in (2.46) of Theorem 1, and $\Psi(q,1)$ is a certain convergent Euler product, found from (3.5) and (3.6). We obtain

$$\Psi(q,1) = \prod_{\substack{p|q \\ p\not\equiv 1 \bmod 4}}\left(1 - \frac{1}{p^2}\right)\prod_{\substack{p|q \\ p\equiv 1 \bmod 4}}\left(\frac{1 + 2^m/(p-1)}{H\left(1/p\right)}\right),$$

which contributes to (3.4) of Theorem 3 and our proof is complete. □

3.4 The upper bound of the coefficients of the polynomial $P_{m,q}(z)$

We now find an upper bound for the coefficients of the polynomial $P_{m,q}(z)$, and show that it depends only on $\log q$ and the number of distinct prime factors of q. We need an upper bound for the coefficients of the polynomial $P_{m,q}(z)$ in chapter 4, when we are estimating a sum over q where the summand includes the polynomial $P_{m,q}(z)$.

Lemma 3.6. *The upper bound for the coefficients*

$$\frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(q,1),$$

of the polynomial $P_{m,q}(z)$ is dependent only on $\log q$ and $\omega = \omega(q)$, the number of distinct prime factors of q.

Proof. We have

$$P_{m,q}(z) = \frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(q,1)z^j,$$

where $V(q,s) = \Psi(q,s)V(s)$ and $V^{(b-j)}(q,1)$ denotes the $(b-j)$-th derivative of $V(q,s)$ evaluated at $s=1$, and

$$\Psi(q,s) = \prod_{\substack{p|q \\ p\not\equiv 1 \bmod 4}} \left(1-\frac{1}{p^{2s}}\right) \prod_{\substack{p|q \\ p\equiv 1 \bmod 4}} \left(1-\frac{e_2}{p^{2s}}+\frac{e_3}{p^{3s}}+\ldots-\frac{e_{2^m}}{p^{2^m s}}\right). \tag{3.14}$$

We consider the derivatives $V^{(b-j)}(q,s)$ where

$$\begin{aligned} V^{(b-j)}(q,s) &= \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^{b-j} \Psi(q,s)V(s) \\ &= \sum_{k=0}^{b-j} {}_{b-j}\mathrm{C}_k \Psi^{(k)}(q,s)V^{(b-j-k)}(s). \end{aligned}$$

This means we can rewrite $P_{m,q}(z)$ as

$$\begin{aligned} P_{m,q}(z) &= \sum_{j=0}^{b} \frac{1}{b!} {}_b\mathrm{C}_j \sum_{k=0}^{b-j} {}_{b-j}\mathrm{C}_k \Psi^{(k)}(q,1)V^{(b-j-k)}(1)z^j \\ &= \sum_{j=0}^{b}\sum_{k=0}^{b-j} \frac{\Psi^{(k)}(q,1)V^{(b-j-k)}(1)z^j}{j!k!(b-j-k)!} \\ &= \sum_{\substack{j \\ j+k\le b}}\sum_{k} \frac{\Psi^{(k)}(q,1)V^{(b-j-k)}(1)z^j}{j!k!(b-j-k)!} \\ &= \sum_{k} \frac{\Psi^{(k)}(q,1)}{k!} \sum_{\substack{j \\ j+k\le b}} \frac{V^{(b-j-k)}(1)z^j}{j!(b-j-k)!}. \end{aligned} \tag{3.15}$$

Since the definition of V(s) in (2.43) does not contain q, the second sum

of (3.15) does not contain q and therefore the coefficient of z^j in $P_{m,q}(z)$ is given by the sum

$$\sum_{j\leq b-k} \frac{V^{(b-j-k)}(1)z^j}{j!(b-j-k)!},$$

which is independent of q, multiplied by the Dirichlet polynomial

$$\sum_{k\leq b} \frac{\Psi^{(k)}(q,1)}{k!},$$

where $j+k\leq b$. Thus we now only have $\Psi^{(k)}(q,1)$ dependent on q. We need to estimate $\Psi^{(k)}(q,s)$ at $s=1$.

The value of $\Psi(q,s)$ does not depend on what power of p divides q, only on whether p divides q. Only those primes p which appear in the prime factorisation of q appear in $\Psi(q,s)$. Let $q=q_1\dots q_\omega$ and $q_a=p_a^{r_a}$ for $a=1,\dots,\omega$. Then

$$\Psi(q,s)=\prod_{a=1}^{\omega}\psi(q_a,s)=\prod_{a=1}^{\omega}\psi(p_a,s).$$

We find the k-th derivative of $\Psi(q,s)$ in terms of $\psi(p_a,s)$,

$$\begin{aligned}\Psi^{(k)}(q,s)&=\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k\prod_{a=1}^{\omega}\psi(p_a,s)\\&=\sum_{\substack{k_1\\k_1+\dots+k_\omega=k}}\cdots\sum_{k_\omega}\prod_{a=1}^{\omega}\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k\psi(p_a,s).\end{aligned}\tag{3.16}$$

We now need to find the k-th derivative of $\psi(p,s)$, replacing the prime p_a with the prime p for ease of notation. We have

$$\psi(p,s)=\begin{cases}P_1\left(\dfrac{1}{p^s}\right) & \text{for } p\equiv 1 \bmod 4,\\[2ex] P_2\left(\dfrac{1}{p^s}\right) & \text{for } p\not\equiv 1 \bmod 4,\end{cases}$$

where we let $M = 2^m$, and

$$P_1\left(\frac{1}{p^s}\right) = \left(1 - \frac{1}{p^s}\right)^{M-1}\left(1 + \frac{M-1}{p^s}\right),$$
$$P_2\left(\frac{1}{p^s}\right) = 1 - \frac{1}{p^{2s}}.$$

The polynomial $P_1\left(1/p^s\right)$ of degree $M = 2^m$ can be expressed as a finite sum

$$\begin{aligned} P_1\left(\frac{1}{p^s}\right) &= 1 + \sum_{t=1}^{M} \frac{(-1)^t}{p^{ts}}\left({}_{M-1}C_t - (M-1)\,{}_{M-1}C_{t-1}\right) \\ &= 1 + \sum_{t=1}^{M} \frac{(-1)^{t-1}(t-1)\,{}_MC_t}{p^{ts}}. \end{aligned} \tag{3.17}$$

To find the k-th derivative of $P_1\left(1/p^s\right)$, we differentiate the form of $P_1\left(1/p^s\right)$ given in (3.17) to obtain

$$\begin{aligned} \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k P_1\left(\frac{1}{p^s}\right) &= \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k \left(1 + \sum_{t=1}^{M} \frac{(-1)^{t-1}(t-1)\,{}_MC_t}{p^{ts}}\right) \\ &= \sum_{t=1}^{M} \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k \left(\frac{(-1)^{t-1}(t-1)\,{}_MC_t}{p^{ts}}\right) \\ &= (-\log p)^k \sum_{t=1}^{M} \frac{(-1)^{t-1}t^k(t-1)\,{}_MC_t}{p^{ts}} \\ &= (-\log p)^k P_3\left(\frac{1}{p^s}\right). \end{aligned} \tag{3.18}$$

We have

$$\begin{aligned} P_3\left(\frac{1}{p^s}\right) &= \sum_{t=1}^{M} \frac{(-1)^{t-1}t^k(t-1)\,{}_MC_t}{p^{ts}} \\ &= -2^k\frac{e_2}{p^{2s}} + 3^k\frac{e_3}{p^{3s}} + \ldots - M^k\frac{e_M}{p^{Ms}}. \end{aligned}$$

Next we find the k-th derivative of $P_2\left(\frac{1}{p^s}\right)$,

$$\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k P_2\left(\frac{1}{p^s}\right) = \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k \left(1 - \frac{1}{p^{2s}}\right) = -\frac{(-2\log p)^k}{p^{2s}}. \tag{3.19}$$

We then estimate the absolute values of the derivatives of (3.18) and (3.19) at $s = 1$. We find

$$\begin{aligned}\left|\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k P_1\left(\frac{1}{p^s}\right)\right|_{s=1} &= \left|(-\log p)^k P_3\left(\frac{1}{p^s}\right)\right|_{s=1} \\ &= (\log p)^k \left|P_3\left(\frac{1}{p}\right)\right|.\end{aligned}$$

We find that

$$\begin{aligned}\left|P_3\left(\frac{1}{p}\right)\right| &= \left|\sum_{t=1}^{M} \frac{(-1)^{t-1} t^k (t-1)_M C_t}{p^t}\right| \\ &\leq \sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{p^t}.\end{aligned}$$

Now as $p \equiv 1 \bmod 4$, we have $p \geq 5$, so that $1/p \leq 1/5$ and $1/p^t \leq 1/5^t$, which means that

$$\sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{p^t} \leq \sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{5^t},$$

and thus

$$\left|\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k P_1\left(\frac{1}{p^s}\right)\right|_{s=1} \leq (\log p)^k \sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{5^t}. \tag{3.20}$$

By the definition of $P_2\left(1/p^s\right)$, we have $p \not\equiv 1 \bmod 4$ so that $p^2 \geq 4$ and $1/p^2 \leq 1/4$, and hence

$$\left|\left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^k P_2\left(\frac{1}{p^s}\right)\right|_{s=1} = \frac{(2\log p)^k}{p^2} \leq 2^{k-2} (\log p)^k. \tag{3.21}$$

We now establish which of the estimates (3.20) and (3.21) is largest. We compare 2^{k-2} with

$$\sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{5^t} = \frac{2^k \ {}_M C_2}{5^2} + \frac{2 \ 3^k \ {}_M C_3}{5^3} + \ldots + \frac{M^k (M-1)}{5^M}.$$

The first term

$$\frac{2^k \ {}_M C_2}{5^2} = \frac{2^{k+m-1}(2^m - 1)}{5^2},$$

is already larger than 2^{k-2} for $m \geq 3$.

Hence, let B be the sum

$$B = \sum_{t=1}^{M} \frac{t^k (t-1)_M C_t}{5^t},$$

so that

$$\left| \left(\frac{\mathrm{d}}{\mathrm{d}s} \right)^k P_1 \left(\frac{1}{p} \right) \right| \leq B(\log p)^k,$$
$$\left| \left(\frac{\mathrm{d}}{\mathrm{d}s} \right)^k P_2 \left(\frac{1}{p} \right) \right| \leq B(\log p)^k,$$

and therefore

$$|\psi^{(k)}(p,1)| \leq B(\log p)^k.$$

We use this with $p = p_a$ and $s = 1$ in (3.16) to find

$$\begin{aligned}
\Psi^{(k)}(q,1) &= \sum_{\substack{k_1 \\ k_1+\ldots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} \left(\frac{\mathrm{d}}{\mathrm{d}s} \right)^k \psi(p_a,1) \\
&\leq \sum_{\substack{k_1 \\ k_1+\ldots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} \left| \left(\frac{\mathrm{d}}{\mathrm{d}s} \right)^k \psi(p_a,1) \right| \\
&\leq \sum_{\substack{k_1 \\ k_1+\ldots+k_\omega=k}} \cdots \sum_{k_\omega} \prod_{a=1}^{\omega} B(\log p_a)^k \\
&\leq B^\omega (\log p_1 + \ldots + \log p_\omega)^k \\
&= B^\omega \left(\log(p_1 \ldots + p_\omega) \right)^k \\
&= B^\omega (\log q)^k. \qquad (3.22)
\end{aligned}$$

We use the estimate $\Psi^{(k)}(q,1) \leq B^{\omega}(\log q)^k$ of (3.22) in (3.15) to find

$$\begin{aligned} P_{m,q}(z) &= \frac{1}{b!}\sum_{j=0}^{b} {}_b\mathrm{C}_j V^{(b-j)}(q,1) z^j \\ &\leq \sum_k \frac{B^{\omega}(\log q)^k}{k!} \sum_{\substack{j \\ j+k\leq b}} \frac{V^{(b-j-k)}(1) z^j}{j!(b-j-k)!} \\ &= B^{\omega} \sum_{\substack{j \\ j+k\leq b}} \sum_k \frac{V^{(b-j-k)}(1)(\log q)^k}{k!j!(b-j-k)!} z^j, \end{aligned}$$

which is dependent only on $\log q$ and $\omega = \omega(q)$, the number of distinct prime factors of q, as required. $\square$

Chapter 4

Cyclic polygons with m integer point vertices

In this chapter we consider cyclic polygons with m integer point vertices which have circumcentres away from the origin, although restricted to the unit square. Firstly we consider those cyclic polygons with m integer point vertices of fixed radius r.

4.1 Lemma bounding the number of cyclic polygons with m integer point vertices which have fixed radius r

Lemma 4. *Let $m \geq 3$ and $q \geq 1$ be fixed integers. Let n be a positive integer such that $q^2 < n$. Let $f(q)$ be the arithmetic function*

$$f(q) = q^2 \prod_{p|q} \left(1 - \frac{1}{p^2}\right) \tag{4.1}$$

which counts pairs of residue classes $a \bmod q$, $b \bmod q$, with highest common factor $(a, b, q) = 1$.

Let $r^* = 4r^*(n, q)$ denote the number of integer points (x, y) on the circle $x^2 + y^2 = n$, with highest common factor $(x, y, q) = 1$. Let $V_m(n, q)$ be the number of cyclic polygons with m integer point vertices, with radius $r = \sqrt{n}/q$, centred at the point $(a/q, b/q)$ in the unit square, where $0 \leq a < q$,

$0 \le b < q$ *and the highest common factor* $(a, b, q) = 1$. *Then*

$$V_m(n, q) \ge f(q)\ {}_lC_m, \tag{4.2}$$

where $l = [r^*/f(q)]$, *the integer part of* $r^*/f(q)$, *and* ${}_lC_m$ *is interpreted as 0 for* $l \le m - 1$.

4.2 Proof of Lemma 4

Let (x, y) be an integer point. Suppose that $(x, y) \equiv (a, b) \bmod q$, with $0 \le a < q$, $0 \le b < q$, so that there exist integers (x_1, y_1) with $x = qx_1 - a$ and $y = qy_1 - b$. The point (x, y) lies on the circle $x^2 + y^2 = n$ if and only if the point (x_1, y_1) lies on the circle

$$\left(x - \frac{a}{q}\right)^2 + \left(y - \frac{b}{q}\right)^2 = \frac{n}{q^2}.$$

We call the integer points (x, y) on the circle $x^2 + y^2 = n$ with highest common factor $(x, y, q) = 1$ the primitive points. Recalling that r^* is the number of integer points on the circle $x^2 + y^2 = n$ with highest common factor $(x, y, q) = 1$, we have that r^* is the total number of primitive points.

Let

$$\sum_a \sum_b{}'$$

denote the sum over pairs of integers (a, b), where $0 \le a < q$, $0 \le b < q$ and highest common factor $(a, b, q) = 1$. Let r^*_{ab} count the primitive points $(x, y) \equiv (a, b) \bmod q$, and since r^* is the total number of primitive points, we have

$$r^* = \sum_a \sum_b{}'\ r^*_{ab}.$$

Let the residue class $(a, b) \bmod q$ be called good if $r^*_{ab} \ge m$, otherwise, for $r^*_{ab} \le m-1$, let the residue class $(a, b) \bmod q$ be called bad. Let B be the number of bad residue classes, and let A be the total number of primitive points in the bad residue classes. Then $A \le (m-1)B \le (m-1)f(q) < r^*$, for $f(q)$ defined in equation (4.1). Let G be the number of good residue classes, and let K be the total number of primitive points in the good residue classes. Then there are $G = f(q) - B$ good residue classes containing $K = r^* - A$ primitive points.

Let

$$C(x) = {}_xC_m = \frac{x}{m!}(x-1)\dots(x-m+1).$$

From each good residue class we can pick primitive points in $C(r^*_{ab})$ ways. The total number of cyclic polygons with m integer point vertices constructed in this way is

$$\sum_{\substack{a \\ (a,b) \text{ good}}} \sum_{b}{}' \; C(r^*_{ab}).$$

To determine a lower bound for this sum we need to use Jensen's inequality (see Hardy, Littlewood and Pólya, chapter 2 [12] or Mitrinović [29]).

Jensen's Inequality. *Let $\varphi(x)$ be a real convex upwards function satisfying $\varphi''(x) \geq 0$ on a closed interval $[a,b]$. Then for $x_1, \dots, x_n$ on $[a,b]$, we have*

$$\sum_{i=1}^{n} \varphi(x_i) \geq n\varphi\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right).$$

The zeros of $C(x)$ lie in the closed interval $[0, m-1]$, so the zeros of $C'(x)$ and $C''(x)$ lie in the open interval $(0, m-1)$. The interval for x will be the closed interval $[m-1, r^*]$, and bad residue classes occur when $r^*_{ab} \in [0, m-2]$, giving $C(r^*_{ab}) = 0$ and $r^*_{ab} \notin [m-1, r^*]$.

We cannot apply Jensen's inequality immediately because of the presence of bad residue classes, which we need to address. The results of Schinzel [35] enable us to continue since they tell us that there must exist some residue class containing $x = r^*_{ab}$ points, with $x \geq r^*/f(q)$.

Let $r^* \geq (m-1)f(q)(f(q)+1)$, so that

$$\frac{r^*}{(B+1)f(q)} \geq \frac{r^*}{f(q)(f(q)+1)} \geq m-1.$$

Then we have the following inequality for $C(x)$,

$$\begin{aligned} C(x) &\geq (B+1)\; P\left(\frac{x}{B+1}\right) \\ &= \frac{x}{m!}\left(\frac{x}{B+1}-1\right)\dots\left(\frac{x}{B+1}-m+1\right). \end{aligned}$$

We replace the B values of $x = r^*_{ab}$, corresponding to bad residue classes, and the one value for which $C(x) = 0$, corresponding to the residue class with no primitive points, with $B+1$ values all equal to $(r^*_{ab})/(B+1)$. For

the other residue classes we do not need to replace any values. We make these changes and return to the sum

$$\sum_{\substack{a \\ (a,b) \text{ good}}} \sum_{b}{}' \; C(r^*_{ab}).$$

We now apply Jensen's inequality to this sum to obtain

$$\begin{aligned}\sum_{\substack{a \\ (a,b) \text{ good}}} \sum_{b}{}' \; C(r^*_{ab}) &\geq \left(\sum_{a \bmod q} \sum_{b \bmod q} 1 \right) \; C \left(\frac{\sum\limits_{a \bmod q} \sum\limits_{b \bmod q} r^*_{ab}}{\sum\limits_{a \bmod q} \sum\limits_{b \bmod q} 1} \right) \\ &= GC\left(\frac{K}{G}\right).\end{aligned}$$

The worst case we have to consider has the K primitive points belonging to the good residue classes (a, b) split evenly between all of the residue classes (a, b), that is, between all of the $f(q)$ residue classes (a, b). This means that each residue class will be good, gives $K = r^*$ and $G = f(q)$ so that we obtain

$$V_m(n, q) = \sum_{\substack{a \\ (a,b) \text{ good}}} \sum_{b}{}' \; C(r^*_{ab}) \geq f(q) C\left(\frac{r^*}{f(q)}\right) \geq f(q)_l C_m,$$

with $l = [r^*/f(q)]$, the integer part of $r^*/f(q)$. In the worst case when the number of primitive points are split evenly between the residue classes, $r^*/f(q)$ is an integer, and $l = r^*/f(q)$.

Hence we have shown that $V_m(n, q) \geq f(q) \; {}_l C_m$, and we are done.

4.3 Bounding the number of cyclic polygons with m integer point vertices with radius $r \leq R$

The result of Theorem 2 gives asymptotic formulae for the number of cyclic polygons with m integer point vertices which have circumcentre at the origin and circumradius at most $\sqrt{N}$. We use the result of Lemma 4 to produce a Theorem which gives a lower bound for the number of cyclic polygons with m integer point vertices with radius $r \leq R$.

There exists a relationship between the number of cyclic polygons with m integer point vertices centred in the unit square with fixed radius $r = \sqrt{n}/q$ and the number of cyclic polygons with m integer point vertices centred in the unit square with radius $r \leq R$, which we now explain.

Lemma 4.1. *Let $V_m(n, q)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with fixed radius $r = \sqrt{n}/q$, and centre of the form $(a/q, b/q)$, where the highest common factor $(a, b, q) = 1$. Let $W_m(R)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with radius $r \leq R$. Then*

$$W_m(R) = \sum_q \sum_n V_m(n, q), \tag{4.3}$$

with $q \leq 6(R+1)^2$ and $n \leq q^2R^2$.

Proof. We have $W_m(R)$ counting all cyclic polygons with m integer point vertices centred in the unit square with radius $r \leq R$, and $V_m(n, q)$ counting the cyclic polygons with m integer point vertices centred in the unit square with radius fixed at $r = \sqrt{n}/q$. Hence $W_m(R)$ is counting all of $V_m(n, q)$ where the fixed radii $r = \sqrt{n}/q$ have size up to radius R. Thus to find $W_m(R)$ we sum $V_m(n, q)$ over n and q. We need limits for our summation.

We find a limit on the size of q by considering the location of the centre of the circle. The centre of the polygons counted by $V_m(n, q)$ is $(a/q, b/q)$. In general, the centre of the circle which passes through three or more integer points (u_i, v_i), $i \geq 3$, has coordinates of the form $(u/D, v/D)$. Thus the centre $(a/q, b/q)$ corresponds to $(u/D, v/D)$, so that $q|D$. The denominator D is given by the determinant

$$D = \begin{vmatrix} u_1 & v_1 & 1 \\ u_2 & v_2 & 1 \\ u_3 & v_3 & 1 \end{vmatrix}.$$

The coordinates of the centre of the circle are found by constructing two chords, one chord between the points (u_1, v_1) and (u_2, v_2), and another chord between the points (u_2, v_2) and (u_3, v_3). The perpendicular bisector of the chord of a circle passes through the centre of the circle, so the intersection of the perpendicular bisector of each of the two chords we constructed will be the centre of the circle.

In $W_m(R)$ each circle has radius at most R, therefore the points (u_i, v_i) satisfy

$$-R \leq u_i < R+1, \quad -R \leq v_i < R+1.$$

When we evaluate the determinant D, we get

$$D = u_1v_2 - u_1v_3 - v_1u_2 + v_1u_3 + u_2v_3 - u_3v_2,$$

which tells us that $D \leq 6(R+1)^2$. As $q|D$, we also have $q \leq 6(R+1)^2$.

We find a limit for n by considering the radius. For $V_m(n,q)$ the radius for our polygons is fixed at $\sqrt{n}/q$, whereas for $W_m(R)$ the radius is less than or equal to R, so that we have $\sqrt{n}/q < R$, which gives $n \leq q^2R^2$. Thus, as in (4.3), $W_m(R)$ is the sum over $V_m(n,q)$ with $n \leq q^2R^2$ and $q \leq 6(R+1)^2$, where these bounds are independent of m. □

In Lemma 4.1 we have $q \leq 6(R+1)^2$. However, large values of q complicate our summation of $V_m(n,q)$ over q, so we prefer to have very small values of q. We know from the result of Lemma 4 that $V_m(n,q) \geq f(q)_l C_m$, where $l = [r^*/f(q)]$ is an integer, $r^* = 4r^*(n,q)$, and $f(q)$ is defined in (4.1).

We recall the definition of $r^*(n,q)$, where $r^*(n,q)$ is the arithmetic function which counts integer solutions of $x^2+y^2 = n$ with $x > 0$, $y \geq 0$ and highest common factor $(x,y,q) = 1$. We need $r^*/f(q)$ to tend towards infinity as R tends towards infinity. We choose q such that $f(q) < r^* = 4r^*(n,q)$. Since the maximum value of $f(q)$ is q^2, this means we choose $q^2 < r^* = 4r^*(n,q)$. Therefore to choose q, we need to consider the size of $r^*(n,q)$.

Lemma 4.2. *The root mean square size estimate for $r^*(n,q)$ is bounded for $n \leq N$, that is*

$$\sqrt{\frac{1}{N}\sum_{n\leq N}(r^*(n,q))^2} \leq \frac{\sqrt{\log N}}{2}.$$

Proof. The results of Section 3.1 tell us that $r^*(n,q) \leq r(n)$ for any value of q, so $r^*(n,q) \leq r(n)$ uniformly in q. Hence,

$$\sum_{n\leq N}(r^*(n,q))^2 \leq \sum_{n\leq N} r^2(n).$$

Ramanujan's estimate [33] gives us

$$\sum_{n\leq N} r^2(n) = \frac{N}{4}\log N + O\left(N^{3/5+\epsilon}\right).$$

Thus our square estimate is

$$\sum_{n\leq N}(r^*(n,q))^2 \leq \frac{N}{4}\log N + O\left(N^{3/5+\epsilon}\right).$$

We divide both sides of the inequality by N to find the mean square estimate,

$$\frac{1}{N}\sum_{n\leq N}(r^*(n,q))^2 \leq \frac{1}{4}\log N + O\left(N^{-2/5+\epsilon}\right).$$

Finally we take the square root of both sides of the inequality to obtain the root mean square size estimate for $r^*(n,q)$,

$$\sqrt{\frac{1}{N}\sum_{n\leq N}(r^*(n,q))^2} \leq \frac{1}{2}\sqrt{\log N} + O\left(\sqrt{N^{-2/5+\epsilon}}\right).$$

We conclude that, in root mean square, $r^*(n,q) \leq \sqrt{\log N}/2$, ignoring the order of magnitude term $O\left(\sqrt{N^{-2/5+\epsilon}}\right)$, which is $o(1)$. □

We use our result on the root mean square size of $r^*(n,q)$ to work out what values q must be restricted to in order to give $q^2 < r^* = 4r^*(n,q)$. We have radius $r \leq R$ and we replace N from Lemma 4.2 with R^2 to give

$$q^2 \leq 4r^*(n,q) \leq 4\frac{\sqrt{\log R^2}}{2} = 2\sqrt{2}\sqrt{\log R} = (8\log R)^{1/2}.$$

This restriction on q^2 is independent of m, the number of integer point vertices of our cyclic polygon. Thus we restrict to small values of q,

$$q \leq (8\log R)^{1/4} < 2(\log R)^{1/4} = Q.$$

We can restrict to these small values of q, $q < Q = 2(\log R)^{1/4}$, since we are calculating a lower bound. We expect that large values of q are extremely rare and can be ignored when we compare q to the root mean square size estimate of $r^*(n,q)$.

We are now ready for the main Theorem of this chapter, concerning the lower bound for the number of cyclic polygons with m integer point vertices centred in the unit square with radius at most R, counted by $W_m(R)$.

4.4 Bounding the number of cyclic polygons with four or more integer point vertices

Theorem 5. *Let $m \geq 4$ be a fixed integer. Let $W_m(R)$ be the number of cyclic polygons with m integer point vertices centred in the unit square with radius $r \leq R$. There exists a polynomial $w(x)$ such that*

$$W_m(R) \geq \frac{4^m}{m!} R^2 \; w(\log R)(1 + o(1)).$$

where $w(x)$ is an explicit polynomial of degree $b = 2^{m-1} - 1$.

Proof. By Lemma 4.1, we have

$$W_m(R) = \sum_{q<6(R+1)^2} \sum_{n \leq q^2 R^2} V_m(n, q),$$

and we restrict q to small values $q < Q = 2(\log R)^{1/4}$, giving a bound of

$$W_m(R) \geq \sum_{q<Q} \sum_{n \leq q^2 R^2} V_m(n, q).$$

By (4.2) this is equivalent to

$$W_m(R) \geq \sum_{q<Q} \sum_{n \leq q^2 R^2} f(q) \; {}_lC_m,$$

with $f(q)$ defined in (4.1), and $l = [r^*/f(q)]$, the integer part of $r^*/f(q)$.

In our proof of Lemma 4 we had

$$V_m(n, q) \geq f(q) C\left(\frac{r^*}{f(q)}\right),$$

and then we bounded this below in terms of l, the integer part of $r^*/f(q)$. Instead let $l_1 = r^*/f(q)$, and then

$$W_m(R) \geq \sum_{q<Q} \sum_{n \leq q^2 R^2} f(q) C(l_1). \tag{4.4}$$

We expand $C(l_1)$, a binomial coefficient, as a function of l_1 to obtain

$$C(l_1) \geq \frac{l_1^m}{m!} - O(l_1^{m-1}).$$

We substitute this into (4.4) to get

$$W_m(R) \geq \sum_{q<Q} \sum_{n \leq q^2R^2} f(q) \frac{l_1^m}{m!} - O\left(\sum_{q<Q} \sum_{n \leq q^2R^2} f(q) l_1^{m-1} \right). \tag{4.5}$$

We consider the first sum in the inequality of (4.5),

$$\begin{aligned} \sum_{q<Q} \sum_{n \leq q^2R^2} f(q) \frac{l_1^m}{m!} &= \sum_{q<Q} \sum_{n \leq q^2R^2} \frac{f(q)}{m!} \left(\frac{r^*}{f(q)} \right)^m \\ &= \frac{1}{m!} \sum_{q<Q} \sum_{n \leq q^2R^2} f(q) \left(\frac{4r^*(n,q)}{f(q)} \right)^m \\ &= \frac{4^m}{m!} \sum_{q<Q} \sum_{n \leq q^2R^2} \frac{(r^*(n,q))^m}{(f(q))^{m-1}}. \end{aligned}$$

Therefore we have

$$W_m(R) \geq \frac{4^m}{m!} \sum_{q<Q} \sum_{n \leq q^2R^2} \frac{(r^*(n,q))^m}{(f(q))^{m-1}} - O\left(\sum_{q<Q} \sum_{n \leq q^2R^2} f(q) l_1^{m-1} \right),$$

and since $f(q) \leq q^2$, we have

$$W_m(R) \geq \frac{4^m}{m!} \sum_{q<Q} \frac{1}{q^{2m-2}} \sum_{n \leq q^2R^2} (r^*(n,q))^m - O\left(\sum_{q<Q} \sum_{n \leq q^2R^2} f(q) l_1^{m-1} \right). \tag{4.6}$$

We now omit the constant factor $4^m/m!$ for ease of notation, and consider the term from (4.6),

$$\sum_{q<Q} \frac{1}{q^{2m-2}} \sum_{n \leq q^2R^2} (r^*(n,q))^m \tag{4.7}$$

We found in Theorem 3 that for large N, as $N \to \infty$,

$$\sum_{n \leq N} (r^*(n,q))^m = N \; P_{m,q}(\log N) + O(q^\epsilon N^{\Phi+\epsilon}), \tag{4.8}$$

where $P_{m,q}(x)$ is a polynomial of degree $b = 2^{m-1} - 1$, whose coefficients depend on q, and Φ is an exponent less than 1, given in (2.2) of Theorem 1. In (4.7) we have $N = q^2R^2$ and we use the expression for the sum over $n \leq N$

of $(r^*(n,q))^m$ in (4.8) to replace the sum of (4.7) with

$$\begin{aligned}
&\sum_{q<Q} \frac{q^2 R^2 \ P_{m,q}(2\log qR)}{q^{2m-2}} + O\left(\sum_{q<Q} \frac{q^{\epsilon}\,(qR)^{2\Phi+2\epsilon}}{q^{2m-2}}\right) \\
=&R^2 \sum_{q<Q} \frac{P_{m,q}(2\log qR)}{q^{2m-4}} + O\left(R^{2\Phi+2\epsilon} \sum_{q<Q} \frac{q^{2\Phi+3\epsilon}}{q^{2m-2}}\right) \\
=&R^2\mathcal{A} + \mathcal{B}. \qquad (4.9)
\end{aligned}$$

We have $\Phi < 1$ and we can assume that ϵ has been chosen so that $2\Phi + 3\epsilon \leq 2$ in $\mathcal{B}$. The sum within the order of magnitude term in $\mathcal{B}$ is of the same size as the sum $\sum 1/q^{\beta}$, with $\beta = 2m-4$, which converges over q with $m \geq 4$. Hence $B = O\left(R^{2\Phi+2\epsilon}\right)$.

We consider the sum in the main term, given by $\mathcal{A}$ in (4.9), with $2m-4$ replaced by β. We write this sum as follows:

$$\sum_{q<Q} \frac{P_{m,q}(2\log qR)}{q^{\beta}} = \sum_{q=1}^{\infty} \frac{P_{m,q}(2\log qR)}{q^{\beta}} + O\left(\sum_{q\geq Q} \frac{P_{m,q}(2\log qR)}{q^{\beta}}\right). \quad (4.10)$$

The polynomial $P_{m,q}$ of degree b has numerical coefficients dependent on both m and q. However, using Lemma 3.6, we found that the upper bound for the coefficients of the polynomial $P_{m,q}(z)$ depends only on $\log q$ and $\omega = \omega(q)$, the number of distinct prime factors of q. Since $q < Q$, $\omega(q)$ is bounded and there exists an absolute constant C with

$$P_{m,q}(2\log qR) \leq C(\log q + \log R)^b,$$

for every q such that $1 \leq q \leq Q$ and $R \geq 10$. Since $m \geq 4$, the exponent β has $\beta = 2m-4 \geq 4$. Hence, by the Integral Test [41], the order of magnitude term from (4.10) becomes

$$\begin{aligned}
O\left(\sum_{q\geq Q} \frac{P_{m,q}(2\log qR)}{q^{\beta}}\right) &= O\left(\int_{Q-1}^{\infty} \frac{(\log q + \log R)^b}{q^{\beta}}\,\mathrm{d}q\right) \\
&= O\left(\frac{\log^b R}{Q^{\beta-1}}\right). \qquad (4.11)
\end{aligned}$$

We consider the main sum of (4.10), which is

$$\sum_{q=1}^{\infty} \frac{P_{m,q}(2\log qR)}{q^{\beta}}. \tag{4.12}$$

The leading term of the polynomial $P_{m,q}(2\log qR)$ is

$$\frac{1}{b!}V(q,1)(2\log qR)^b = \frac{2^b}{b!}V(1)\Psi(q,1)(\log q + \log R)^b,$$

where $\Psi(q,1)$ comes from the expression for $\Psi(q,s)$ evaluated at $s=1$. We recall that $M = 2^m$, and we have

$$\begin{aligned}\Psi(q,s) &= \prod_{\substack{p|q \\ p\not\equiv 1 \bmod 4}} \left(1-\frac{1}{p^{2s}}\right) \prod_{\substack{p|q \\ p\equiv 1 \bmod 4}} \left(1-\frac{1}{p^{2s}}\right)^M \left(1+\frac{M}{p^s-1}\right) \\ &= \sum_{\substack{d=1 \\ p|d \Rightarrow p|q}}^{\infty} \frac{e(d)}{d^s}.\end{aligned}$$

In the summation form of $\Psi(q,s)$, $e(d)=0$ unless d is powerful. This series absolutely converges at $s=1$. The coefficients $e(d)$ are integers, possibly negative, with $e(p^r)$ bounded and $e(1)=1$. For $p \equiv 1 \bmod 4$, $e(p)=0$, $e(p^r) = (-)1^{r-1}(r-1)_M C_r$ for $r = 2,\ldots,M$, and $e(p^r)=0$ for $r \geq M+1$. For $p \not\equiv 1 \bmod 4$, $e(p)=0$, $e(p^2)=-1$, and $e(p^r)=0$ for $r \geq 3$.

Thus the main sum of (4.10) given in (4.12) is

$$\sum_{q=1}^{\infty} \frac{2^b}{b!}\frac{V(1)\Psi(q,1)}{q^{\beta}}(\log q + \log R)^b$$

plus the sum over q of lower order terms of $P_{m,q}(2\log qR)$, which is greater than or equal to

$$\frac{2^b\ V(1)}{b!}\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^{\beta}}(\log q + \log R)^b.$$

This is a polynomial in $\log R$ of degree b,

$$\begin{aligned}
&\frac{2^b\ V(1)}{b!}\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^\beta}(\log q+\log R)^b\\
=&\frac{2^b\ V(1)}{b!}\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^\beta}\sum_{i=0}^{b}\ {}_bC_i\ \log^i q\ \log^{b-i} R\\
=&\frac{2^b\ V(1)}{b!}\sum_{i=0}^{b}\ {}_bC_i\ \log^{b-i} R\sum_{q=1}^{\infty}\frac{\Psi(q,1)\log^i q}{q^\beta}. \qquad (4.13)
\end{aligned}$$

Now

$$\frac{\mathrm{d}}{\mathrm{d}\beta}\left(\frac{1}{q^\beta}\right)=\frac{-\log q}{q^\beta},$$

and

$$\left(-\frac{\mathrm{d}}{\mathrm{d}\beta}\right)\frac{1}{q^\beta}=\frac{\log q}{q^\beta}.$$

Hence (4.13) becomes

$$\begin{aligned}
&\frac{2^b\ V(1)}{b!}\sum_{i=0}^{b}\ {}_bC_i\ \log^{b-i} R\sum_{q=1}^{\infty}\Psi(q,1)\left(-\frac{\mathrm{d}}{\mathrm{d}\beta}\right)^i\frac{1}{q^\beta}\\
=&\frac{2^b\ V(1)}{b!}\sum_{i=0}^{b}\ {}_bC_i\ \log^{b-i} R\left(-\frac{\mathrm{d}}{\mathrm{d}\beta}\right)^i\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^\beta}. \qquad (4.14)
\end{aligned}$$

We have $0<\Psi(q,1)<\Upsilon d(q)$ where

$$\Upsilon=\prod_{\substack{p|q\\ p\equiv 1 \bmod 4\\ p\le M-1}}\left(1+\frac{M-1}{p}\right),$$

and $d(q)$ is the divisor function counting the positive divisors of q. Hence

$$\sum_{q=1}^{\infty}\frac{\Psi(q,1)}{q^\beta}<\Upsilon\sum_{q=1}^{\infty}\frac{d(q)}{q^\beta},$$

and in (4.14)

$$\left(-\frac{\mathrm{d}}{\mathrm{d}\beta}\right)^i \sum_{q=1}^{\infty} \frac{\Psi(q,1)}{q^\beta} < \left(-\frac{\mathrm{d}}{\mathrm{d}\beta}\right)^i \Upsilon \sum_{q=1}^{\infty} \frac{d(q)}{q^\beta}$$
$$= \Upsilon \left| \left(\frac{\mathrm{d}}{\mathrm{d}s}\right)^i \zeta^2(s) \right|_{s=\beta}. \qquad (4.15)$$

The sum over q in (4.14) is bounded by the result of (4.15), and since

$$\Psi(q,1) = \sum_{\substack{d=1 \\ p|d \Rightarrow p|q}}^{\infty} \frac{e(d)}{d}$$

forms a convergent series of positive terms, $\Psi(q,1)$ converges to a positive constant. The constant will involve the i-th derivative of $\zeta^2(\beta)$ and we denote it by $\mathcal{K}_i(\beta)$. We therefore have

$$\sum_{q=1}^{\infty} \frac{P_{m,q}(2\log qR)}{q^\beta} \geq w(\log R) = \frac{2^b\ V(1)}{b!} \sum_{i=0}^{b}\ {}_bC_i\ \mathcal{K}_i(\beta)\ \log^{b-i} R, \quad (4.16)$$

where the polynomial $w(\log R)$ is of degree b.

We have shown using (4.11) and (4.16) that the main sum in (4.10) satisfies

$$\mathcal{A} = \sum_{q<Q} \frac{P_m^*(2\log qR)}{q^\beta} \geq w(\log R) + O\left(\frac{\log^b R}{Q^{\beta-1}}\right).$$

Returning to the expression in (4.9), we have

$$R^2\mathcal{A} + \mathcal{B} \geq R^2\ w(\log R) + R^2 O\left(\frac{\log^b R}{Q^{\beta-1}}\right) + O\left(R^{2\Phi+2\epsilon}\right).$$

Since $2\Phi + 2\epsilon < 2\Phi + 3\epsilon \leq 2$, we find $2\Phi + 2\epsilon < 2$ which makes our error term $O\left(R^{2\Phi+2\epsilon}\right) = o(1)$. As the polynomials $P_{m,q}(x)$ and $w(x)$ have positive numerical leading coefficients,

$$O\left(\frac{\log^b R}{Q^{\beta-1}}\right) = O\left(\frac{w(\log R)}{Q^{\beta-1}}\right) = w(\log R)\, O\left(\frac{1}{Q^{\beta-1}}\right),$$

and

$$O\left(\frac{1}{Q^{\beta-1}}\right) = o(1),$$

for our choice of $\beta = 2m-4$ with $m \geq 4$. We therefore have

$$R^2\mathcal{A} + \mathcal{B} \geq R^2\ w(\log R)\,(1+o(1)) + o(1) = R^2\ w(\log R)\,(1+o(1))\,. \quad (4.17)$$

We now need to consider the order of magnitude term from (4.5) involving the sum over l_1^{m-1}, which is

$$\begin{aligned} & O\left(\sum_{q<Q}\sum_{n\leq q^2R^2} f(q) l_1^{m-1}\right) \\ = \ & O\left(\sum_{q<Q}\frac{1}{(f(q))^3}\sum_{n\leq q^2R^2}(r^*(n,q))^{m-1}\right) \\ = \ & O\left(\sum_{q<Q}\frac{1}{(f(q))^{m-2}}\left(q^2R^2\ P_{m-1,q}(2\log qR) + O\left(q^{\epsilon}(qR)^{2\Phi+2\epsilon}\right)\right)\right). \quad (4.18) \end{aligned}$$

Now

$$\frac{1}{(f(q))^{m-2}} = O\left(\frac{1}{q^{2m-2}}\right),$$

and since we are already in an order of magnitude term, we ignore the $O\left(q^{\epsilon}(qR)^{2\Phi+2\epsilon}\right)$ term of (4.18) to get

$$O\left(R^2\sum_{q<Q}\frac{q^2}{q^{2m-2}}\ P_{m-1,q}(2\log qR)\right).$$

This is of the same form as $\mathcal{A}$ in (4.9). Thus we have

$$O\left(R^2\sum_{q<Q}\frac{P_{m-1,q}(2\log qR)}{q^{2m-4}}\right) = O\left(w_1(\log R)(1+o(1))\right), \quad (4.19)$$

where here $w_1(\log R)$ is a polynomial in $\log R$ of degree $b_{m-1} = 2^{m-2}-1$. We conclude that

$$\begin{aligned} W_m(R) &\geq \sum_{q<Q}\sum_{n<q^2R^2} V_m(n,q) \\ &\geq \frac{4^m}{m!}R^2\ w(\log R)(1+o(1)), \end{aligned}$$

since the order of magnitude term from (4.19) will be dominated by the order of magnitude term from (4.17), and we are done. □

Part II

The distribution of domains and different configurations of the circle

Chapter 5

Definitions and History of Domains and Configurations

We now consider questions linked to the distribution of different configurations of the integer points of the circle passing through the unit square. We examine whether different configurations of points are distributed uniformly throughout the unit square for circles of fixed radius. Results are obtained by looking at the distribution of the crossing points of circles, which form the boundaries of domains.

5.1 Definition of Configuration and Domain

We begin by defining configurations and domains of configurations for a general oval, S. Let S be a closed convex plane shape, called an oval, with a sufficiently smooth boundary curve C, and area A. The oval S has a designated centre at the origin. An S-oval $S(r, P)$ is formed by magnifying S by a factor r and then translating the centre from the origin to the point P.

Definition. The configuration $J(r, P)$ is the set of integer points inside the set $S(r, P)$, $J(r, P) = \{(m, n) \in S(r, P)\}$, where (m, n) are points of the integer lattice.

A configuration is called a screen image when considering problems associated with machine vision. The pixels of a computer screen are treated as the points (m, n) of the integer lattice. The two configurations $J(r, P)$ of the S-oval $S(r, P)$ and $J(r', P')$ of the S-oval $S(r', P')$ are equivalent if $J(r', P')$

is a translation of $J(r, P)$ by an integer vector. The size of the configuration $J(r, P)$ is $N(r, P)$, the number of integer points in $J(r, P)$.

Definition. The domain $D(J)$ of the configuration $J(r, P)$ is the set of possible positions of the centre of the oval $S(r, P)$ within the configuration $J(r, P)$ such that $N(r, P)$ and $J(r, P)$ remain the same.

We fix our shape S to be a circle, where $S(R, (u, v))$ denotes the position of the circle S in the plane such that the centre of S is (u, v), not necessarily a lattice point, and the radius of S is R, with R sufficiently large enough to ensure that $S(R, (u, v))$ always contains at least one point (m, n) of the integer lattice. The boundary curve of $S(R, (u, v))$ will be denoted as $C(u, v)$. We want to find the size of the configurations of a circle as for a domain to be defined we need to know the number of integer points in a configuration.

5.2 History of the Circle Problem

The method of counting squares for estimating the area of a closed curve begins with placing a piece of transparent squared paper over the curve to allow for the count, with each square a lattice unit apart. We count a square when its lower left corner lies within or on the circle. These are the crossing points of the lattice contained within the curve. For the circle of radius R, when R is an r-digit number, the estimate for the area of the circle will have about $2r$ decimal digits. The Circle Problem asks how many of these digits are significant. The main stages in the history of this problem are as follows.

1. Counting squares inside the circle, to an accuracy of the number of squares cut by the circle. The number of integer points inside or on the circle of radius R centred at the origin is $N(R, (0, 0)) = \pi R^2 + D(R, (0, 0))$, where $D = D(R, (0, 0))$ is the discrepancy between the area of the circle πR^2 and the actual number of points $N(R, (0, 0))$. A basic estimate for D is $O(R+1)$, used by Gauss in "De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem" [8] that gives his name to the Gauss circle problem. This method shows that about r digits are significant.

2. Diophantine Approximation, approximating the circle by a polygon whose sides have rational gradients, as in the work of Voronoï [39] and Sierpiński [36]. This shows that about $4r/3$ digits are significant.

The polygon has vertices P_1, P_2, ..., P_k, $P_{k+1} = P_1$, where $P_i = (m_i, n_i)$ and the gradient of the side P_iP_{i+1} is the rational a_i/q_i such that

$$\frac{a_i}{q_i} = \frac{n_{i+1} - n_i}{m_{i+1} - m_i}.$$

In an undergraduate research project, Bayer [1], was asked to count configurations of circles with small fixed radius. As part of the project, Bayer looked at approximating the circle by a polygon. Bayer considered a side P_iP_{i+1} of a polygon where the line equation $f(x)$ of the side was $f(x) = (a_ix + b_i)/q_i$. Bayer found that the number of points N_i under the side P_iP_{i+1} of a polygon was

$$N_i = \frac{a_i}{q_i} \sum_{n=m_i}^{m_{i+1}-1} n + (P_{i+1} - P_i + 1)\left(\frac{2b_i - q_i}{2q_i} + t\frac{1}{2}\right).$$

The total number of integer points under the polygon is found by adding and subtracting N_i for $i = 1, \ldots, k+1$ as appropriate.

3. Fourier series and exponential sums. Van der Corput [38] was the first to use Fourier series correctly, again showing that about $4r/3$ digits are significant. Van der Corput went on to give an extremely complicated iterative method, which gives about $(2 - \kappa)r$ digits of significance for various values of $\kappa < 2/3$. The simplest form of this iteration has been optimised, but the general form is a branched iteration, so complicated that most results claimed from using it are disputed [10]. This method was generally only applied to simple explicit cases like the circle.

4. The Bombieri-Iwaniec-Mozzochi method, which combines ideas 2 and 3 with many technical tricks, and uses a general 'large sieve' inequality to bound error terms in mean fourth power. The method was developed by Iwaniec and Mozzochi [26], based on the work of Bombieri and Iwaniec [3] on exponential sums. It is advantageous because it introduces number-theoretic ideas to the problem.

   Iwaniec and Mozzochi's method was equivalent to approximating the circle (or hyperbola) by a polygon whose sides had rational gradient, as Voronoï [39] and Sierpiński [36] had done, and then estimating exponential sums, one sum for each side of the polygon, in the mean fourth power. This method showed that about $15r/11$ digits are significant.

The Bombieri-Iwaniec-Mozzochi method was the most successful so far, avoiding some of the shortcomings associated with the individual methods. The problem with the Fourier series method is estimating often complicated exponential sums and the problem with Diophantine Approximation is the restriction to rational gradients for the sides of the polygons. However, the Bombieri-Iwaniec-Mozzochi method does possess both these problems, and elegant new ideas had to be brought in.

The Bombieri-Iwaniec-Mozzochi method was first simplified, and then elaborated, by Huxley in order to obtain slightly sharper results. Huxley adapted the method to treat general oval curves and made small improvements to show that about $(2-\kappa)r$ digit are significant for certain values of $\kappa < 7/11$.

We quote Huxley's most recent version of the bound (Theorem 2 of [17]) using the notation for a circular disc given by Huxley in [24], where $B(R,(a,b))$ is the circular disc centred at (a,b) with radius R.

Theorem 5.1. *The number of integer points inside a disc $B(R,(a,b))$ can be estimated as*

$$N(R,(a,b)) = \pi R^2 + O(R^{\kappa}(\log R)^{\lambda}). \tag{5.1}$$

with $\kappa = 131/208$ and $\lambda = 18627/8320$.

5. Kendall [27] considered the effect of moving the circle, $B(R,(a,b))$ in the notation used for Theorem 5.1, or oval, relative to the square lattice of integer points. There is a variable discrepancy or error term $D(R,(a,b))$. The discrepancy is a function $D(u,v)$ of position, periodic in u and v with period 1, so that $D(R,(a,b))$ has a Fourier series. Kendall found the Fourier series in x and y for $D(R,(x,y))$, and deduced that about $3r/2$ digits were significant for almost all positions (x,y). Using Kendall's displacement Fourier series [27], it turns out that the Fourier coefficient for the circle works out exactly as a Bessel integral function, and gives the Voronoï- Hardy-Landau formula. Thus

$$D = R\sum_{n=1}^{\infty} \frac{r(n)}{\sqrt{n}} J_1(2\pi R\sqrt{n}),$$

where $r(n)$ is the number of representations of the integer n as the sum of two squares.

5.3 Results on configurations

When counting squares, Žunić asked for the actual sets of squares counted, how they changed under translation, and how to use these patterns in computer vision and film animation. Eventually, results were forthcoming in collaboration with Huxley ([19, 22–25]). A digital disc is the binary picture or digitisation of a circle. A digital disc for Žunić is the union of the squares counted, but for Huxley it is the set of integer points indexing these squares, that is, the set of all integer points inside the circle. We use Huxley's concept that a digital disc is the set of all integer points inside the circle.

Huxley and Žunić collaborated in [23] to find a theorem which counts the number of different digitisations of discs having radius R.

Theorem 5.2. (*Huxley and Žunić [23]*)
There are $4\pi R^2 + O(R^{\kappa+1}(\log R)^{\lambda})$ different (up to translation) digitisations of discs having radius R.

Huxley and Žunić additionally consider the number of different digital discs containing N points, and their main result in [24] counts these discs.

Theorem 5.3. (*Huxley and Žunić [24]*) *The number of different (up to translation) digital discs consisting of N integer points satisfies*

$$D_N \leq 4N + O(N^{(\kappa+1)/2}(\log N)^{\lambda}). \tag{5.2}$$

The study of configurations was further developed by Huxley and Žunić in [22, 25]. Let $K(R)$ be the number of equivalence classes of configurations with $r = R$ fixed, let $L(n)$ be the number of equivalence classes of configurations with $N(r, P) = n$ fixed, and let $M(N)$ be the number of equivalence classes of configurations with $1 \leq N(r, P) \leq N$. The screen size $N(r, P)$ is asymptotic to Ar^2 as $r \to \infty$, where A is the area of S. Huxley and Žunić found estimates of $L(n)$, $M(N)$, and $K(r)$ for a closed convex shape S in the plane with smooth boundary curve C and area A under different conditions, which we now state.

Smoothness Condition. The boundary C is made up of c_0 pieces, on each of which there is a radius of curvature ρ, continuously differentiable with respect to the direction ψ of the tangent, with

$$c_1 \leq \rho \leq c_2, \quad \left| \frac{\mathrm{d}\rho}{\mathrm{d}\psi} \right| \leq c_3,$$

where c_0, c_1, c_2 and c_3 are constants with c_0 a positive integer, $0 < c_1 \leq 1$, and $c_2 \geq 1$.

Triangle Condition (for a particular r). There is no point P where the boundary curve $C(r, P)$ of $S(r, P)$ passes through three or more integer points.

Quadrangle Condition. There is no size r and no point P where $C(r, P)$ passes through four or more integer points.

Theorem 5.1 also holds for an S-oval satisfying the Smoothness Condition, with the constant π for circles replaced by the area constant A. The result of Huxley and Žunić in [25] bounds $K(r)$, with an area constant B.

Theorem 5.4. (*Huxley and Žunić* [25]) *Let S be strictly convex. Then as $r \to \infty$,*

$$K(r) \leq Br^2 + O(r). \tag{5.3}$$

If S satisfies the Triangle Condition, then

$$K(r) = Br^2 + O(r). \tag{5.4}$$

If S satisfies the Smoothness Condition, then (5.3) *holds with an error term of the same form as in* (5.1)*, and so does* (5.4) *if S satisfies both conditions.*

Huxley and Žunić then gave bounds for $L(n)$ and $M(N)$ in [22].

Theorem 5.5. (*Huxley and Žunić [22]*) *Let S be convex. Then for all $n \geq 1$, $N \geq 1$, $L(n) \leq 2n-1$ and $M(N) \leq N^2$. If S satisfies the Quadrangle Condition, then $L(n) = 2n - 1$ and $M(N) = N^2$.*

Huxley and Žunić found that in the general case where $L(n) = 2n - 1$, $M(N) = N^2$, $K(r) + 1$ is the screen size of $T(r, O)$, where T is the Brunn-Minkowski difference set of S, and O is the origin. Thus $K(r)$ was found to be asymptotic to Br^2, where B is the area of T.

Huxley and Žunić then worked with Kolountzakis in [19], and the results of Huxley, Žunić and Kolountzakis are more general. Huxley, Kolountzakis and Žunić in [19] investigate the special cases where there are fewer configurations of domains, which makes $K(r)$, $L(n)$ and $M(N)$ are smaller. They answer the question of what conditions on the boundary curve C of S enable an estimate of the number of configurations. They prefer local conditions which can be verified to non-local conditions such as the Triangle and Quadrangle condition. The local conditions give some overall results, and this approach enables improvement of the upper bound in (5.3) of Theorem 5.4 from $O(r)$ to $O(r^{\kappa}(\log r)^{\lambda})$. Huxley, Kolountzakis and Žunić then introduce the Level 4 Smoothness Condition which leads to the main result of [19].

Level 4 Smoothness Condition. The boundary curve C has a radius of curvature ρ, twice continuously differentiable with respect to the direction ψ of the tangent, with the Smoothness Condition holding, and also

$$\left| \frac{\mathrm{d}^2\rho}{\mathrm{d}\psi^2} \right| \leq c_4,$$

for some constant c_4.

Theorem 5.6. (*Huxley, Kolountzakis and Žunić [19]*) *Let S satisfy the Level 4 Smoothness Condition. If θ is a real number such that*

$$K(r) = Br^2 + O(r^{\theta})$$

holds as $r \to \infty$, then $\theta \geq 1/2$.

Huxley, Kolountzakis and Žunić then consider examples which satisfy some of the conditions we have discussed but not all conditions, or which fail to satisfy the conditions for certain values of r, which are the square roots of rational numbers. The most familiar example which fails to satisfy certain conditions is the circle. We know that there exist circles passing through five or more integer points, so the circle does not satisfy the quadrangle condition, and the triangle condition also fails, for some values of r. The bounds of Part I show that circles passing through five or more integer points are rare.

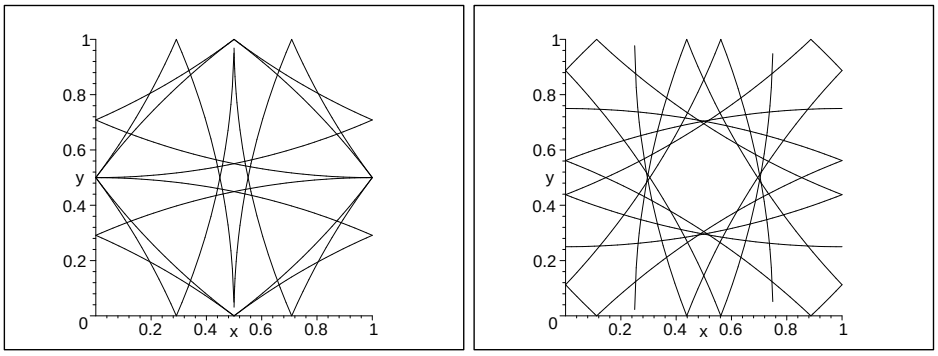
We want to find the size of the configurations of a circle. We have an estimate, due to Huxley and Žunić, for how many different configurations there are. Domains can be shifted to the unit square using equivalent configurations which translate the circle's centre by an integer vector. The config-

urations are the same modulo the integer lattice. The position of the integer points relative to each other distinguishes the configuration, not the position of the points themselves on the lattice. It is possible that a domain can become disconnected as the radius R increases when two opposite boundary arcs, concave with respect to the domain, expand to touch and cross, but this is extremely rare.

5.4 Domain diagrams and the distribution of domains

In order to be able to examine the distribution of domains, we need to introduce the domain diagram. Domains are bounded by the arcs of circles of radius R with centres at various integer points. A domain diagram shows where these arcs of circles meet the unit square. We give examples of domain diagrams in Figure 5.1. These are not typical because they show multiple intersections, but a typical example has domains too small to see on a printed page.

Figure 5.1: Examples of Domain Diagrams

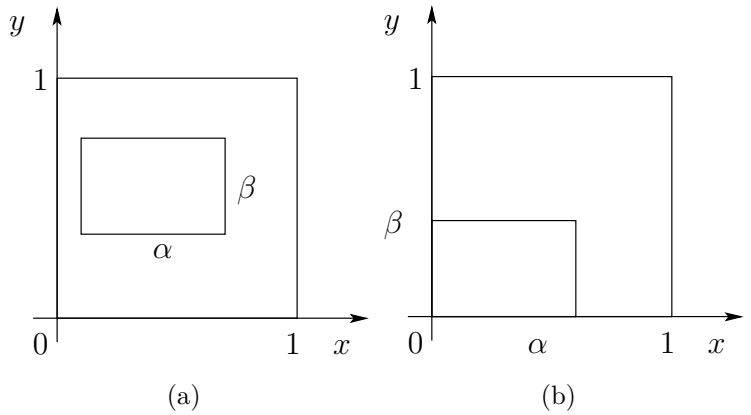


(a) Domain Diagram for $R = 2.5$ (b) Domain Diagram for $R = 2.75$

The domain $D(J)$ of a configuration J is a bounded set. We drop the radius from our notation as we consider a fixed radius in our main discussion. The average area of domains is approximately $1/(4\pi R^2)$, so most domains are smaller than this, and clearly all domains are small. We find an upper bound for the size of a domain, of $O\left(1/\sqrt{R}\right)$.

The theory of uniform distribution modulo 1 was introduced by Weyl [40]. We state here the version of Weyl's criterion given in [5], which says that a

Figure 5.2: Rectangles



necessary and sufficient condition for a sequence $s_1, s_2, \ldots$ of real numbers to be uniformly distributed modulo 1, is that for each integer $l \neq 0$,

$$S(N) = \frac{1}{N} \sum_{n=1}^{N} e(l\ S_n) \to 0,$$

as $N \to \infty$, where $e(l\ S_n) = \exp(2\pi i\ l\ S_n)$. Weyl's work proved that this was equivalent to bounds for exponential sums formed from the sequence, which showed that Diophantine approximation results were closely related to the general problem of cancellation in exponential sums, which occurs throughout analytic number theory in the bounding of error terms.

We investigate what happens to the distribution of domains in the unit square. We look at how many domains meet in the rectangle contained within the unit square, shown in Figure 5.3(a), where the rectangle has sides of length α in the x direction and β in the y direction such that $0 < \alpha < 1$ and $0 < \beta < 1$. Without loss of generality we can take the origin $(0, 0)$ as a corner of the rectangle, so that we have the rectangle with corner co-ordinates of $(0, 0)$, $(\alpha, 0)$, (α, β) and $(0, \beta)$, depicted in Figure 5.3(b).

The distribution of domains in the general rectangle, G, of Figure 5.3, which does not have the origin as a corner, can be found by considering other rectangles which do have the origin as a corner and adding and subtracting the number of domains in these rectangles, as demonstrated in Figure 5.4.

We count the vertices of domains where the arcs meet rather than count the domains themselves. Counting corners of domains in a box is the same as counting pairs of circles whose centres satisfy some relationship, so that

Figure 5.3: General rectangle

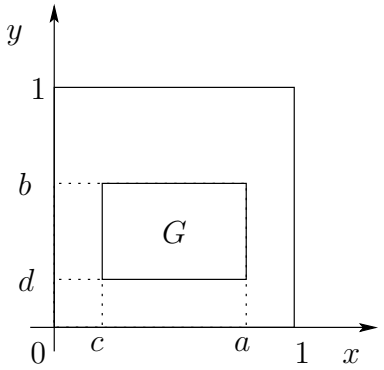
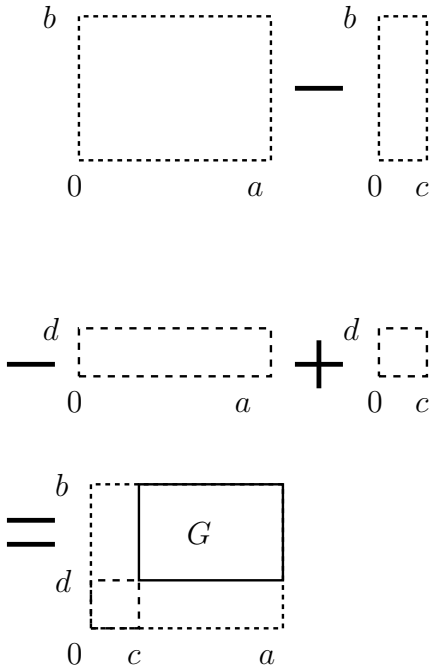


Figure 5.4: Adding and subtracting rectangles



we are counting integer points in some region in 4-dimensional space, as in the work of Huxley and Žunić [23].

Let $G(\alpha, \beta)$ be the rectangle with the lower left corner at the origin and with sides of length α in the x-direction, and β in the y-direction. Let $C(m, n)$ be the translation of $C(R, (0, 0))$ by the integer vector (m, n), and let $C(m', n')$ be the translation of $C(R, (0, 0))$ by the integer vector (m', n'). We are interested in the arcs $C(m, n)$ and $C(m', n')$, which pass within the rectangle $G(\alpha, \beta)$. We find an analogue for the rectangle of Huxley and Žunić's Lemma 3.1, which counts the number of intersections of arcs $C(m, n)$ and $C(m', n')$ according to multiplicity in the unit square. We then find the number of regions of the rectangle $G(\alpha, \beta)$ which are formed by domain boundaries, and show that they are uniformly distributed.

Chapter 6

Domain calculations - bounding domains and the critical strip

6.1 Bounding domains

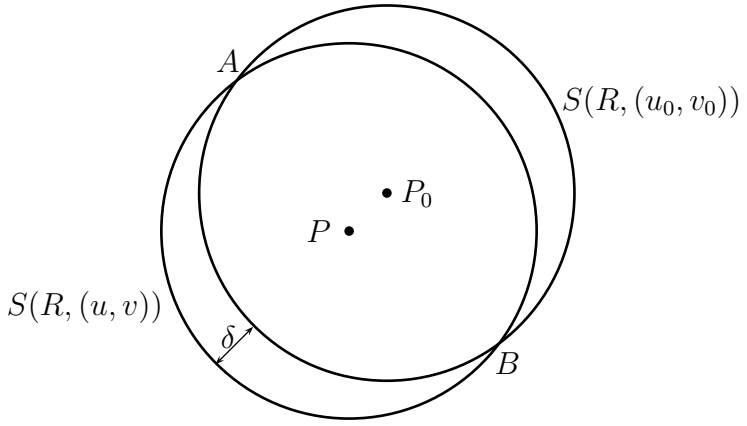
Lemma 6.1. *Domains have size at most $O(1/\sqrt{R})$ in any direction.*

Proof. Let (u, v) and (u_0, v_0) be in the same domain D, so that the two circles centred at $P = (u, v)$ and $P_0 = (u_0, v_0)$, both with radius R, contain the same set of integer points. Then all integer points are contained in the intersection of the two circles, the lens $S(R, (u, v)) \cap S(R, (u_0, v_0))$, illustrated in Figure 6.1. Thus there must be at least one integer point in the intersection of the two circles since configurations are non-empty sets. Also the crescents $S(R, (u, v)) \setminus S(R, (u_0, v_0))$ and $S(R, (u_0, v_0)) \setminus S(R, (u, v))$ will not contain any integer points.

We now estimate the maximum width, δ, of the each of the two crescents $S(R, (u, v)) \setminus S(R, (u_0, v_0))$ and $S(R, (u_0, v_0)) \setminus S(R, (u, v))$ in Figure 6.1. By symmetry, the maximum width will be the same for both crescents. We begin by drawing a circle through the two points A and B where the circles intersect, which has diameter AB. Since AB is the common chord of two circles of radius R, we know that the length of AB is at most $2R$.

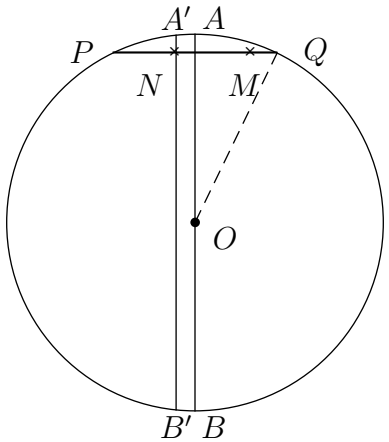
We examine the lattice line $A'B'$ closest to the diameter AB and take the last integer point on this line lying inside the circle, and we call this point N. We then move along the lattice line at right angles from $A'B'$ to the last integer point inside the circle, and we call this point M. The points of intersection of the circle with the lattice line that M lies on are denoted by

Figure 6.1: The intersection of two domains



P and Q, depicted in Figure 6.2. If there are no points on the lattice line perpendicular to $A'B'$ that enable us to do this, then we move to the next nearest lattice line perpendicular to $A'B'$ possessing such points, and apply the method just described.

Figure 6.2: Circle with diameter AB



The results of Huxley in [16] indicate that if a strip is placed around a smooth curve, where the curve is not too steep, then for a "thick" enough curve, there will be an integer point in the strip. We need to find out how

far M is from the circumference of the circle to find out the strip's maximum width. We do this by calculating the length of the line OM and finding the difference between the length OM and the radius of the circle. We initially assume the strip contains a horizontal or vertical part of the circle, and then we treat the case where this does not hold.

We want the maximum value for the diameter $AB \leq 2R$, so we take $AB = 2R$, to give the radius $OQ = R$. Now $A'B'$ is almost a diameter with $A'N < 1$, so let $A'B' \doteq 2R$. We use Pythagoras' Theorem to obtain $R^2 = (OQ)^2 = (OD)^2 + (DQ)^2$ and $(OM)^2 = (OD)^2 + (DM)^2$. These rearrange to give $(OM)^2 = R^2 + (DM)^2 - (DQ)^2$. Since $MQ < 1$, we have $DQ = DM + O(1)$, giving $DM = DQ - O(1)$, and thus

$$(OM)^2 = R^2 + (DQ - O(1))^2 - (DQ)^2 = R^2 + O(DQ + 1).$$

Now D is the midpoint of the line PQ, and by choice of N, $DN < 1$, so $(DQ)^2 \doteq PN \times NQ$. By the intersecting chords theorem (Euclid, book 3, prop. 35) [7], $PN \times NQ = A'N \times NB'$, and as $A'N < 1$ and $NB' < 2R$ we have $PN \times NQ < 2R$. This gives $(DQ)^2 < 2R$ and hence $DQ < \sqrt{2R}$. Thus we have

$$(OM)^2 = R^2 + O(\sqrt{R}) = R^2 \left(1 + O\left(\frac{1}{R^{3/2}}\right)\right),$$

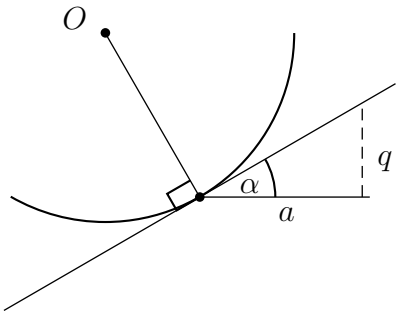
and so the length OM satisfies

$$OM = R + O\left(\frac{1}{\sqrt{R}}\right).$$

The distance between the point M and the circumference of the circle is the difference between the radius of the circle R and the length OM, which is $O(1/\sqrt{R})$.

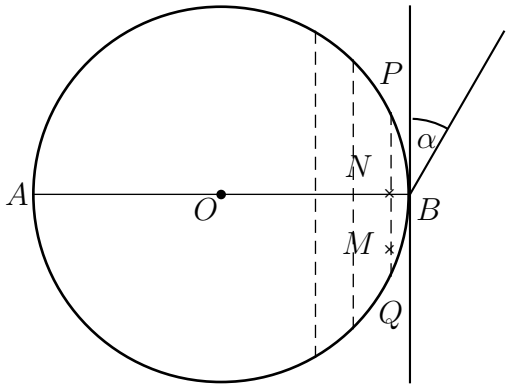
We now treat the case where a strip is taken around part of the circle which does not include a vertical or horizontal part of the circumference. We take a tangent to the circle in the middle third of the strip, where the tangent has small rational height a/q in its lowest terms, giving $\tan\alpha = a/q$ as in Figure 6.3. The radius perpendicular to the tangent with direction vector $(a, -q)$ is then constructed. We consider the lattice lines parallel to the tangent vector (q, a), which are at a distance $1/\sqrt{a^2 + q^2}$ apart. We approach the circumference of the circle towards the tangent along the radius drawn from the centre of the circle O, and choose the last lattice line that

Figure 6.3: Arc of circle and its tangent



intersects the radius before we reach the circumference. We denote this lattice line by the dotted line PQ in Figure 6.4. Lattice points on this line are $\sqrt{a^2+q^2}$ apart. We choose the last integer point before the lattice line goes outside of the circle, and call this M as shown in Figure 6.4.

Figure 6.4: Circle corresponding to a strip round part of it



In this case, we use the diameter AB itself and N, the midpoint of PQ. Then $PN = NQ$ so that $(NQ)^2 = AN \times NB$. We have

$$R^2 = (OQ)^2 = (ON)^2 + (NQ)^2 \quad \text{and} \quad (OM)^2 = (ON)^2 + (NM)^2.$$

By definition, we have $NB < 1/\sqrt{a^2+q^2}$ and $MQ < \sqrt{a^2+q^2}$. This gives

$$\begin{aligned}(NM)^2 &= (NQ - \sqrt{a^2+q^2})^2 \\ &= (NQ)^2 - 2\sqrt{a^2+q^2}NQ + a^2 + q^2 \\ &= (NQ)^2 + O(NM - 1).\end{aligned}$$

We have $AB = 2R$, so that $AN \doteq 2R$, meaning $(NQ)^2 < 2R$, and $NQ <$

$\sqrt{2R}$. As before, we find

$$(OM)^2 = (ON)^2 + (NM)^2 = R^2 - (NQ)^2 + (NM)^2 = R^2 + O(\sqrt{R}).$$

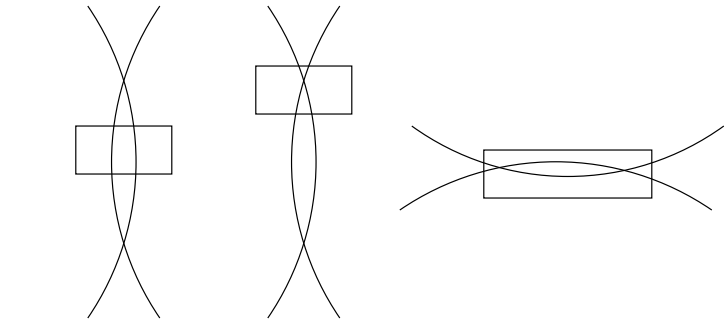
Thus the distance of the point M from the circle will again be $O(1/\sqrt{R})$.

The number of integer points in the strip needs to be zero for the crescents in Figure 6.1 to be empty of lattice points. We now know that there are integer points within a distance $O(1/\sqrt{R})$ of the circumference of the circle which has radius R. Therefore the distance between the circumferences of two circles of radius R with centres P and P_0 which form the crescents of Figure 6.1 must be less than $O(1/\sqrt{R})$. The maximum width of the strip, δ, is the same as the distance between the centres P and P_0. Therefore the distance between the centres P and P_0 is at most $O(1/\sqrt{R})$, and domains have size at most $O(1/\sqrt{R})$ in any direction. □

6.2 Critical points and the critical strip: how many domains meet the rectangle?

Domain boundaries are arcs of circles of radius R with centres at integer points. The domain boundaries that meet the rectangle do not necessarily have intersections with other domains inside the boundary of the rectangle. Intersecting domains may intersect within the rectangle not at all; or intersecting domains may have intersection points either once or twice within the rectangle, as demonstrated in Figure 6.5.

Figure 6.5: Ways that intersections of domains can intersect within the rectangle



A) Not at all B) Once C) Twice

Domain boundaries are arcs of circles of radius R with centres at integer

points. These centres are at a distance exactly R from some point in the rectangle since the arc of the circle passes through the rectangle, and they are referred to as critical points. Hence a critical point is the integer point which is at a distance exactly R from some point in the rectangle. The centres that give domain boundaries in the rectangle are a subset of the centres that give domain boundaries in the unit square.

Huxley and Žunić find a bound in [23] for the number of critical points of the unit square of $8R + O(R^\kappa(\log R)^\lambda)$. Thus, there are a maximum of $8R+O(R^\kappa(\log R)^\lambda)$ circles used to draw domain boundaries and each of these boundaries cuts the edge of the unit square. This also gives an upper bound for the number of critical points of the rectangle.

Hence the number of circles used to draw domain boundaries in our rectangle $G(\alpha, \beta)$ is at most $8R+O(R^\kappa(\log R)^\lambda) = O(R)$. The number of circles which cut the boundary of the rectangle is the same as the number of circles used to draw domain boundaries and is thus also $O(R)$. We can also think of this as having $O(R)$ edges of domains cutting the boundary of the rectangle, or the boundary of the rectangle cutting $O(R)$ domains.

The critical strip $\mathcal{E}$ is the area where the critical points for the rectangle can be found. We find it by drawing four circles of radius R centred at the points $(0, 0)$, $(\alpha, 0)$, (α, β) and $(0, \beta)$, which are the corners of our rectangle. Let $\mathcal{E}_1$ be the area where all of these circles intersect i.e. the common area shared by each of the four circles, bounded by four arcs. The first arc belongs to the circle centred at $(0, 0)$, drawn between the points

$$\left(\sqrt{R^2 - \frac{\beta^2}{4}}, \frac{\beta}{2}\right) \quad \text{and} \quad \left(\frac{\alpha}{2}, \sqrt{R^2 - \frac{\alpha^2}{4}}\right).$$

The second arc belongs to the circle centred at $(\alpha, 0)$, drawn between the points

$$\left(\frac{\alpha}{2}, \sqrt{R^2 - \frac{\alpha^2}{4}}\right) \quad \text{and} \quad \left(\alpha - \sqrt{R^2 - \frac{\beta^2}{4}}, \frac{\beta}{2}\right).$$

The third arc belongs to the circle centred at (α, β), drawn between the points

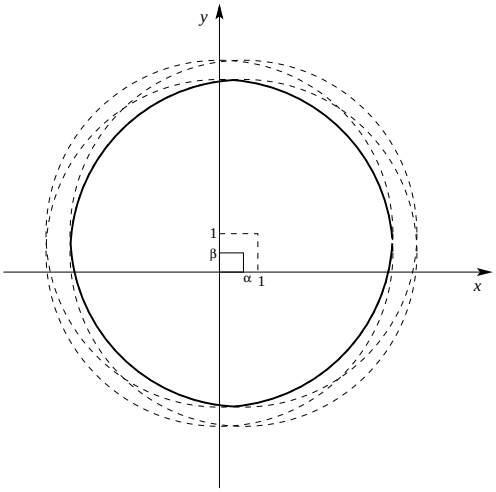
$$\left(\alpha - \sqrt{R^2 - \frac{\beta^2}{4}}, \frac{\beta}{2}\right) \quad \text{and} \quad \left(\frac{\alpha}{2}, \beta - \sqrt{R^2 - \frac{\alpha^2}{4}}\right),$$

and the fourth arc belongs to the circle centred at $(0, \beta)$, drawn between the

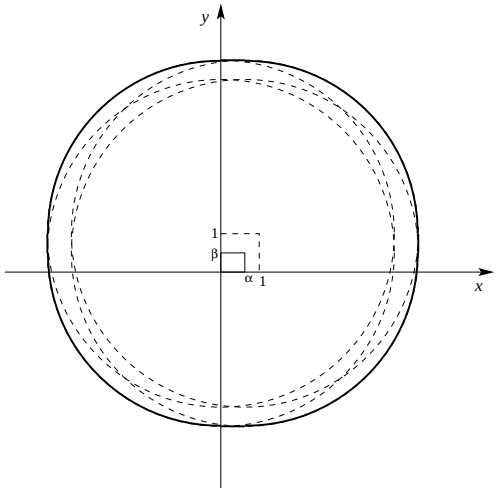
points

$$\left(\frac{\alpha}{2}, \beta - \sqrt{R^2 - \frac{\alpha^2}{4}}\right) \quad \text{and} \quad \left(\sqrt{R^2 - \frac{\beta^2}{4}}, \frac{\beta}{2}\right).$$

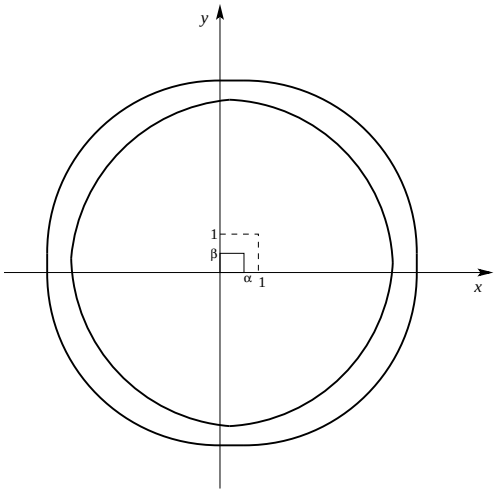
Figure 6.6: The critical strip and its components



(a) The area $\mathcal{E}_1$ inside the bold line



(b) The area $\mathcal{E}_2$ inside the bold line



(c) The critical strip $\mathcal{E}$ between the bold lines

Let $\mathcal{E}_2$ be the area which contains the areas of all of the circles. $\mathcal{E}_2$ is bounded by four lines and four arcs. The first line runs from $(\alpha + R, 0)$ to $(\alpha + R, \beta)$, and the first arc runs from $(\alpha + R, \beta)$ to $(\alpha, \beta + R)$, belonging to the circle centre (α, β). The second line runs from $(\alpha, \beta + R)$ to $(0, \beta + R)$, and the second arc runs from $(0, \beta + R)$ to $(-R, \beta)$, belonging to the circle centre $(0, \beta)$. The third line runs from $(-R, \beta)$ to $(-R, 0)$, and the third arc

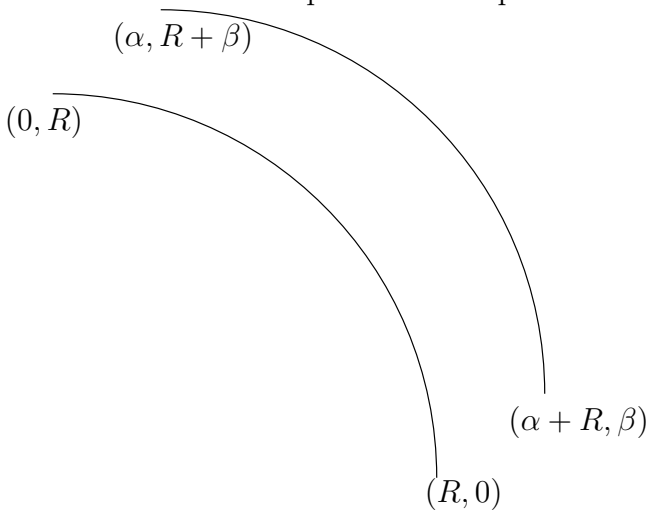
runs from $(-R, 0)$ to $(0, -R)$, belonging to the circle centre $(0, 0)$. Lastly, the fourth line runs from $(0, -R)$ to $(\alpha, -R)$, and the fourth arc runs from $(\alpha, -R)$ to $(\alpha + R, 0)$, belonging to the circle centre $(\alpha, 0)$. The critical strip $\mathcal{E}$ is found by subtracting the area $\mathcal{E}_1$ from the area $\mathcal{E}_2$, giving $\mathcal{E} = \mathcal{E}_2 \backslash \mathcal{E}_1$. All three of the areas $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}$ can be seen in Figure 6.6.

6.3 The area of the critical strip

Lemma 6. *The area of the critical strip is* $4R(\alpha + \beta) + O(\alpha\beta)$.

Proof. The critical strip can be covered by four rectangles, where each rectangle has area $\alpha\beta$, and four curved strips, which are each bounded by two quadrants of circles. Overlap occurs only in the bounded regions of the rectangles. The area of the critical strip is the sum of the area of the four curved strips $+ O(\alpha\beta)$, where the order of magnitude term is obtained from the area of the rectangles.

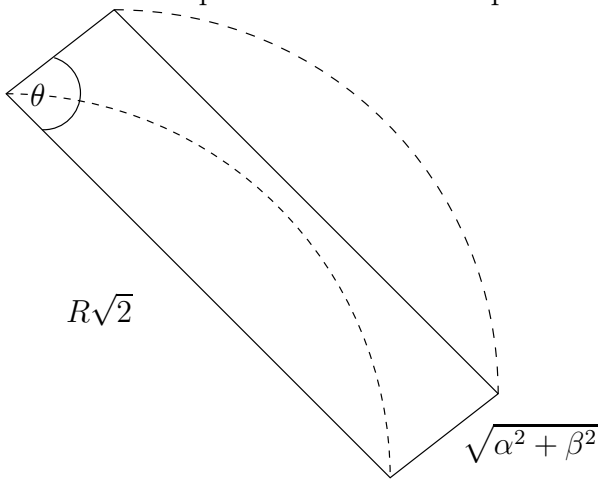
Figure 6.7: The curved strip in the first quadrant



We now find the area of one curved strip, the strip based in the first quadrant with x and y positive (see Figure 6.7). This strip is found between the arc of the circle centre $(0, 0)$, radius R, drawn from $(0, R)$ to $(R, 0)$ and the arc of the circle centre (α, β), radius R, drawn from $(\alpha + R, \beta)$ to $(\alpha, \beta + R)$. The distance between the two arcs is $\sqrt{\alpha^2 + \beta^2}$, and the straight line distance between the two end points of an arc is $R\sqrt{2}$. In Figure 6.8, we

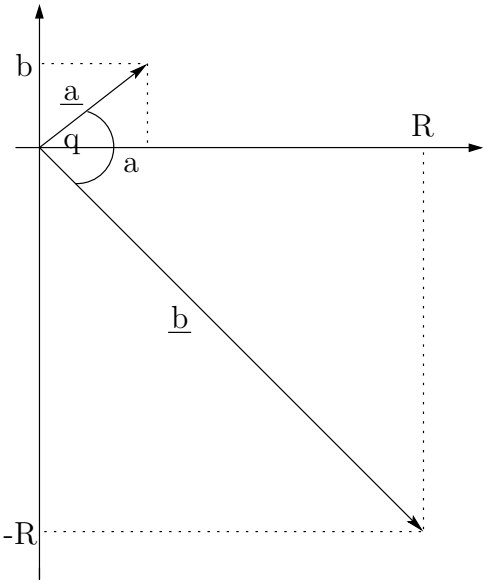
show how we transform our curved strip into a parallelogram with sides of length $\sqrt{\alpha^2+\beta^2}$ and $R\sqrt{2}$.

Figure 6.8: The curved strip transformed into a parallelogram



We use vector calculus to find the area of the parallelogram. Let $\underline{a} = \alpha\underline{i} + \beta\underline{j}$ and $\underline{b} = R\underline{i} + (\beta - R)\underline{j}$ with an angle θ between the vectors $\underline{a}$ and $\underline{b}$, and we have $|\underline{a}| = \sqrt{\alpha^2+\beta^2}$ and $|\underline{b}| = R\sqrt{2}$. These vectors are shown in Figure 6.9. The magnitude of $-\underline{a} \times \underline{b}$ is the same as the area of our

Figure 6.9: Vector diagram



parallelogram,

$$-\underline{a} \times \underline{b} = \begin{bmatrix} -\alpha & -\beta \\ R & -R \end{bmatrix} = \alpha R + \beta R = R(\alpha + \beta),$$

so that the area of our parallelogram is $R(\alpha + \beta)$. Hence the area of the curved strip in the first quadrant is $R(\alpha + \beta)$. The area of the critical strip is four times the area of the curved strip with error $O(\alpha\beta)$, so that the area of the critical strip is $4R(\alpha + \beta) + O(\alpha\beta)$. □

We now state Proposition 2.1 of [23], which is a special case of Theorem 5 of [17], which we reproduced earlier in Theorem 5.1.

Proposition 6.1. *Let S be a plane region bounded by c_1 arcs with the following smoothness property. There is a length scale $R \geq 2$ and positive constants c_2, c_3 and c_4 such that on each arc, when we regard the radius of curvature ρ as a function of the tangent angle ψ, then*

$$c_2 R \leq \rho \leq c_3 R, \quad \left| \frac{\mathrm{d}\rho}{\mathrm{d}\psi} \right| \leq c_4 R.$$

Then the number of integer points in S is

$$AR^2 + O(c_1 R^\kappa (\log R)^\lambda)$$

where A is the area constant associated with S so that AR^2 is the area of S. The values of κ and λ are our standard values, $\kappa = 131/208$ and $\lambda = 18627/8320$. The constant c_1 in the O-notation is constructed from the constants c_2, c_3 and c_4.

Taking the set S in Proposition 6.1 to be $S(R, (a, b))$, the circle of radius R centred at the point $P = (a, b)$, we will have $N(P) = \pi R^2 + O(c_1 R^\kappa (\log R)^\lambda)$ regardless of the position of P within the rectangle $G(\alpha, \beta)$. The straight sections of the boundary of $\mathcal{E}$ can be replaced by circular arcs of radius R without altering the set of integer points in $\mathcal{E}$, so Proposition 6.1 combined with Lemma 6 giving the area of the critical strip tells us that the number of critical points for our rectangle $G(\alpha, \beta)$ is $4R(\alpha + \beta) + O(R^\kappa (\log R)^\lambda)$.

Chapter 7

Positions of arcs cutting the rectangle

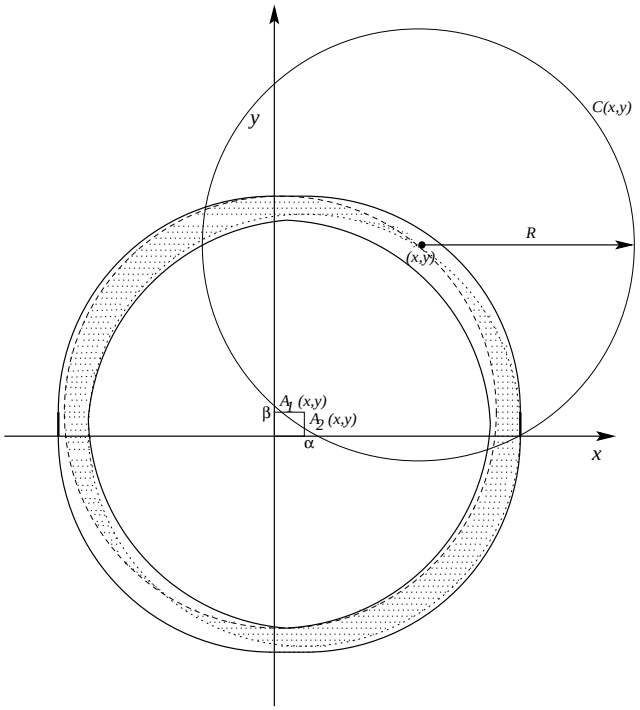
We are interested in finding analogues for the rectangle of Huxley and Žunić's Lemma and Theorem, which count the number of intersections of domains in the unit square. In order to do this, we need to locate where the arcs which form domain boundaries intersect with the rectangle, and estimate their partial derivatives and radius of curvature as contour lines of a function.

7.1 Locating arcs which cut the rectangle

To locate the arcs which form domain boundaries intersecting with the rectangle, we begin by drawing the circle $C(m,n)$ centred at (m,n) with radius R, for each critical point (m,n). The arc $C(m,n)$ will cut the boundary of the rectangle at two points which we denote as $A_1(m,n)$ and $A_2(m,n)$. We estimate the number of multiple crossings of the two arcs $C(m,n)$ and $C(m',n')$ within the rectangle. In the rare case where the arcs $C(m,n)$ and $C(m',n')$ cross twice in the rectangle $G(\alpha,\beta)$, the points $A_1(m,n)$ and $A_2(m,n)$ both lie outside the arc $C(m',n')$. This occurs when $m' = -m + O(\alpha), \quad n' = -n + O(\beta)$. The bound for the number of critical points for the rectangle implies that there are $O(R)$ pairs of arcs which cross twice. If $C(m,n)$ and $C(m',n')$ cross once inside the rectangle $G(\alpha,\beta)$, then the points $A_1(m,n)$ and $A_2(m,n)$ lie on opposite sides of the arc $C(m',n')$.

Let $E_1(m,n)$ be the subset of the critical strip $\mathcal{E}$ consisting of those points

Figure 7.1: The set $E(x, y)$



which lie inside the circle $S(A_1, (m, n))$, and outside the circle $S(A_2, (m, n))$,

$$E_1(m, n) = \mathcal{E} \cap \{S(A_1, (m, n)) \backslash S(A_2, (m, n))\}.$$

Similarly, let $E_2(m, n)$ be the subset of the critical strip $\mathcal{E}$ consisting of those points which lie inside the circle $S(A_2, (m, n))$ and outside the circle $S(A_1, (m, n))$,

$$E_2(m, n) = \mathcal{E} \cap (S(A_2, (m, n)) \backslash S(A_1, (m, n))).$$

When the arc $C(m, n)$ crosses the arc $C(m', n')$, then the point (m', n') lies in $E(m, n)$, where $E(m, n)$ is the union of the sets $E_1(m, n)$ and $E_2(m, n)$, so that $E(m, n) = E_1(m, n) \cup E_2(m, n)$.

For any point (x, y) in the critical strip $\mathcal{E}$, not necessarily an integer point, we consider the arc $C(x, y)$, the set $E(x, y)$, the point $A_1(x, y)$, and the point $A_2(x, y)$, given by the same construction as used when (x, y) is a critical point (m, n), illustrated in Figure 7.1. The set $E(x, y)$ is bounded by the dotted and dashed lines, which are the circumferences of two circles of radius R whose centres are at a distance $d(x, y)$ apart, where $d(x, y)$ is the

distance between the two points $A_1(x, y)$ and $A_2(x, y)$. Let $e(x, y)$ be the area of $E(x, y)$. The area $e(x, y)$ is the shaded region in Figure 7.1.

In the following discussion, we write d for $d(x, y)$, A_1 for $A_1(x, y)$ and so on. When we fix d, there are still many possible positions for A_1 and A_2 on the perimeter of our rectangle. The more common cases are where the points A_1 and A_2 are on adjacent sides of the rectangle, called corner cuts (Figure 7.2); and where the points A_1 and A_2 are on opposite sides of the rectangle, called side cuts (Figure 7.4). There is a rare case where both the points A_1 and A_2 lie on the same side of the rectangle, called a same-side cut (Figure 7.5). It is also possible, although extremely unlikely, for the domain boundary to make a four-point cut, cutting the perimeter of the rectangle four times (Figure 7.6).

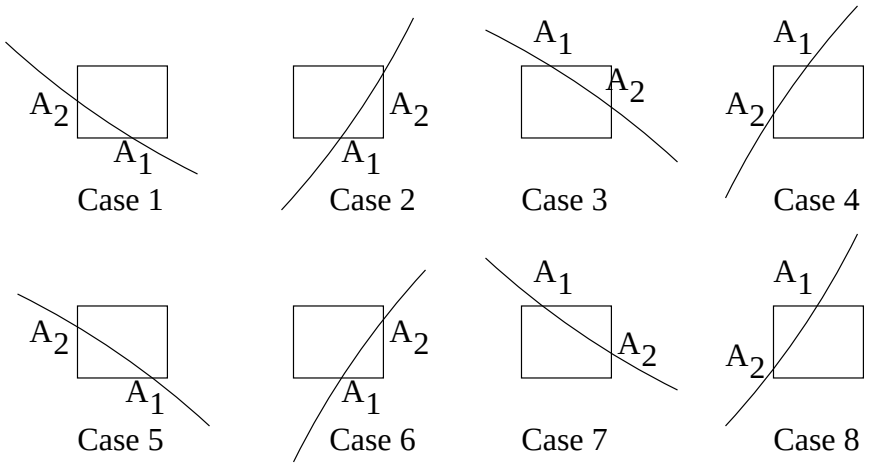
Let $\theta < \pi/2$ be the angle formed between the x-axis and the line A_1A_2. The angle of inclination of the line A_1A_2 is measured anticlockwise from the positive x-axis. When the angle of inclination is less than $\pi/2$, then θ and the angle of inclination are the same. When the angle of inclination is greater than $\pi/2$, then θ is the difference between π and the angle of inclination. We use the angle θ to parameterise the contour lines of the area $e(x, y)$. We wish to estimate the partial derivatives and radius of curvature for the contour lines of $e(x, y)$ to use in our results of Chapter 8.

7.2 Arcs cutting adjacent sides of the rectangle

First we consider where the points A_1 and A_2 are on adjacent sides of the rectangle, the corner cuts. So far we have not distinguished the points A_1 and A_2. For corner cuts we make the convention that A_1 lies on a horizontal side of the rectangle, and A_2 lies on a vertical side. There are eight types of corner cut when we take account of the orientation of the domain boundary. There are four corners, and for each corner there are two possible orientations for the arc A_1A_2 (Figure 7.2).

Lemma 7.1. *The contour lines formed by arcs cutting adjacent sides of the rectangle have radius of curvature ρ approximately R. Let the angle ψ, as usual, denote the direction of the tangent vector, then also in all corner cut cases we find that* $\mathrm{d}\rho/\,\mathrm{d}\psi$ *is* $O(R)$.

Figure 7.2: Corner cuts



Proof We take the cases in pairs, considering case i and case $i+4$ together, $1 \leq i \leq 4$. The same two points A_1 and A_2 on adjacent sides of the rectangle come from two possible centres X and X' for the circular arc A_1A_2, which lie on the perpendicular bisector of the line segment A_1A_2 (Figure 7.3). The equation of the perpendicular bisector is

$$y - y_0 = \frac{-1}{m}(x - x_0), \tag{7.1}$$

where (x_0, y_0) denotes the midpoint M of A_1A_2, and m denotes the gradient of A_1A_2.

The angle $\phi = \widehat{MXA_1}$ is determined by $\sin\phi = d/2R$. To work backwards from A_1 and A_2 to find the centres X and X', we draw the circle centre M radius $R\cos\phi$ to cut the perpendicular bisector of A_1A_2 at X and X'.

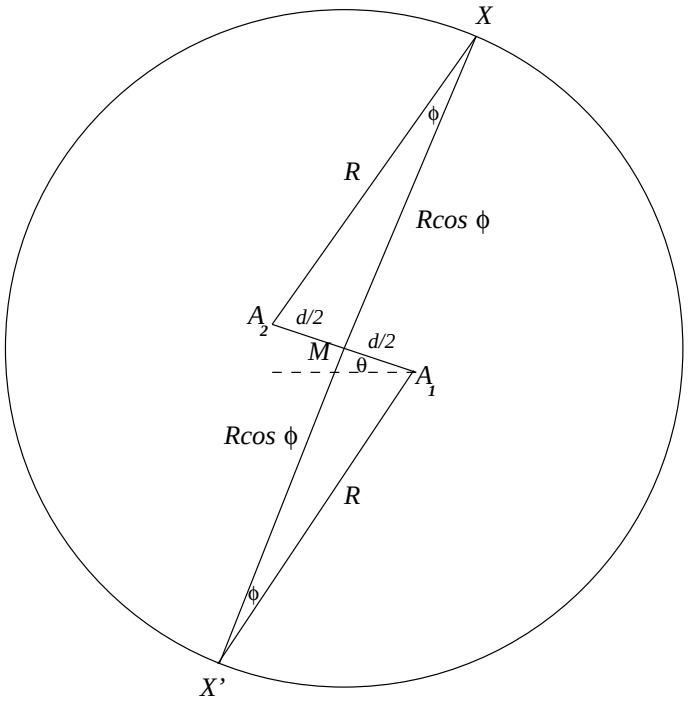
We give the construction for cases 1 and 5, when $A_1 = (d\cos\theta, 0)$ and $A_2 = (0, d\sin\theta)$, so that the midpoint $M = (1/2\, d\cos\theta, 1/2\, d\sin\theta)$, and the gradient of A_1A_2 is $-\tan\theta$. Hence we substitute into (7.1) to find

$$y = x\cot\theta + \frac{d}{2}\sin\theta - \frac{d}{2}\cos\theta\cot\theta. \tag{7.2}$$

The equation of the circle with centre M and radius $R\cos\phi$ is

$$\left(x - \frac{d}{2}\cos\theta\right)^2 + \left(y - \frac{d}{2}\sin\theta\right)^2 = (R\cos\phi)^2. \tag{7.3}$$

Figure 7.3: Concepts



We substitute (7.2) for y in (7.3) and use $d = 2R\sin\phi$, so that

$$x = \pm R\cos\phi\sin\theta + \frac{d}{2}\cos\theta = \pm R\sin\left(\theta \pm \phi\right). \tag{7.4}$$

We then substitute (7.4) into (7.2) to obtain $y = \pm R\cos\left(\theta \mp \phi\right)$. Hence the two possible points X and X' have coordinates

$$\left(\pm R\sin\left(\theta \pm \phi\right), \pm R\cos\left(\theta \mp \phi\right)\right), \tag{7.5}$$

where the upper signs are taken together. Since d is fixed, the angle ϕ is fixed, and the area $e(x, y)$ is fixed. As the angle θ varies, the point (x, y) moves along a contour line of the function $e(x, y)$.

We must show that this part of the contour has radius of curvature approximately R. The points X and X' differ only by the sign in (7.5). We consider case 1, for ease of notation, in which

$$(x, y) = \left(R\sin(\theta + \phi), R\cos(\theta - \phi)\right).$$

The tangent vector at this point is

$$\left(\frac{\mathrm{d}x}{\mathrm{d}\theta}, \frac{\mathrm{d}y}{\mathrm{d}\theta}\right) = \left(R\cos(\theta+\phi), -R\sin(\theta-\phi)\right), \tag{7.6}$$

and the arc length s satisfies,

$$\begin{aligned}\left(\frac{\mathrm{d}s}{\mathrm{d}\theta}\right)^2 &= \left(\frac{\mathrm{d}x}{\mathrm{d}\theta}\right)^2 + \left(\frac{\mathrm{d}y}{\mathrm{d}\theta}\right)^2 \\ &= R^2\left(\cos^2(\theta+\phi) + \sin^2(\theta-\phi)\right) \\ &= R^2\left(1 - \sin 2\phi \sin 2\theta\right),\end{aligned}$$

which gives

$$\frac{\mathrm{d}s}{\mathrm{d}\theta} = R\left(1 - \sin 2\phi \sin 2\theta\right)^{1/2}. \tag{7.7}$$

Let the angle ψ, as usual, denote the direction of the tangent vector in (7.6). Then

$$\tan\psi = -\frac{\sin(\theta-\phi)}{\cos(\theta+\phi)} = \frac{\tan\phi - \tan\theta}{1 - \tan\phi\tan\theta},$$

and

$$\tan\theta + \tan\psi = \frac{\sin\phi\cos 2\theta}{\cos\phi\cos(\theta+\phi)}. \tag{7.8}$$

We calculate

$$\tan(\theta+\psi) = \frac{\tan\theta + \tan\psi}{1 - \tan\theta\tan\psi}. \tag{7.9}$$

In (7.8) we have an expression for the numerator of (7.9) in terms of θ and ϕ. We now transform the denominator of (7.9),

$$\begin{aligned}1 - \tan\theta\tan\psi &= 1 + \frac{\sin(\theta-\phi)\sin\theta}{\cos(\theta+\phi)\cos\theta} \\ &= \frac{\cos(\theta+\phi)\cos\theta + \sin(\theta-\phi)\sin\theta}{\cos(\theta+\phi)\cos\theta} \\ &= \frac{\cos\phi - \sin\phi\sin 2\theta}{\cos(\theta+\phi)\cos\theta}.\end{aligned} \tag{7.10}$$

Our expressions in (7.8) and (7.10) now have the same denominator, which will cancel when the expressions are substituted into (7.9), and thus will give

$$\tan(\theta+\psi) = \frac{\sin\phi\cos 2\theta}{\cos\phi - \sin\phi\sin 2\theta}.$$

Hence

$$\psi = -\theta + \tan^{-1}\left(\frac{\sin\phi\cos 2\theta}{\cos\phi - \sin\phi\sin 2\theta}\right), \tag{7.11}$$

and

$$\begin{aligned}\frac{\mathrm{d}\psi}{\mathrm{d}\theta} &= -1 + \frac{\sin 2\phi\sin 2\theta - 2\sin^2\phi}{\sin 2\phi\sin 2\theta - 1} \\ &= \frac{2\cos^2\phi - 1}{\sin 2\phi\sin 2\theta - 1} \\ &= \frac{-\cos 2\phi}{1 - \sin 2\phi\sin 2\theta}.\end{aligned} \tag{7.12}$$

We obtain the radius of curvature ρ from the results of (7.7) and (7.12),

$$\begin{aligned}\rho &= \left|\frac{\mathrm{d}s}{\mathrm{d}\psi}\right| = \left|\frac{\mathrm{d}s/\,\mathrm{d}\theta}{\mathrm{d}\psi/\,\mathrm{d}\theta}\right| \\ &= R(1 - \sin 2\phi\sin 2\theta)^{1/2}\left|\frac{1 - \sin 2\phi\sin 2\theta}{-\cos 2\phi}\right| \\ &= R\frac{(1 - \sin 2\phi\sin 2\theta)^{3/2}}{|\cos 2\phi|},\end{aligned}$$

which means that

$$\begin{aligned}\rho &= \frac{R\,(1 - \sin 2\phi\sin 2\theta)^{3/2}}{|\cos 2\phi|} \\ &= \frac{R\,(1 - O(\phi))^{3/2}}{1 - O(\phi)} \\ &= R + O(d) \\ &\asymp R.\end{aligned} \tag{7.13}$$

We need to check that the derivative

$$\frac{\mathrm{d}\rho}{\mathrm{d}\psi} = \frac{\mathrm{d}\rho/\,\mathrm{d}\theta}{\mathrm{d}\psi/\,\mathrm{d}\theta} \tag{7.14}$$

is continuous and has order of magnitude $O(R)$ or smaller.

We already know the derivative of ψ with respect to θ, given in (7.12). Since we have ρ expressed in terms of θ in (7.13) we can find the derivative of ρ with respect to θ directly from this expression,

$$\frac{\mathrm{d}\rho}{\mathrm{d}\theta} = -3R\tan 2\phi\cos 2\theta(1 - \sin 2\phi\sin 2\theta)^{1/2}. \tag{7.15}$$

We substitute (7.15) and (7.12) into (7.14) to obtain

$$\frac{\mathrm{d}\rho}{\mathrm{d}\psi} = 3R\tan 2\phi \sec 2\phi \cos 2\theta (1 - \sin 2\phi \sin 2\theta)^{3/2}.$$

This is continuous except where $\cos 2\phi = 0$. Since R is supposed to be large, and $d \leq \sqrt{\alpha^2 + \beta^2} \leq \sqrt{2}$, and $\sin\phi = d/2R$, then ϕ is a small angle and $\cos 2\phi$ is non-zero. The order of magnitude of this derivative is at most R, the size suggested by dimensional analysis.

We performed these calculations and estimates for case 1 of the corner cuts. The other seven cases will be similar, so that the radius of curvature in all cases is approximately R. Case 5 differs from case 1 only by sign changes. In cases 2 and 6, $A_1 = (\alpha - d\cos\theta, 0)$ and $A_2 = (\alpha, d\sin\theta)$, so that the midpoint $M = (\alpha - 1/2\, d\cos\theta, 1/2\, d\sin\theta)$, and the two possible points X and X' have coordinates

$$\left(\pm R\sin\left(\theta \mp \phi\right) + \alpha, \mp R\cos\left(\theta \pm \phi\right)\right),$$

where the upper signs are taken together. When we differentiate with respect to θ to obtain the tangent vector, α disappears, and the tangent vector is

$$\left(\pm R\cos\left(\theta \mp \phi\right), \pm R\sin\left(\theta \pm \phi\right)\right).$$

This tangent vector differs only by sign changes from that of case 1.

In cases 3 and 7, $A_1 = (\alpha - d\cos\theta, \beta)$ and $A_2 = (\alpha, \beta - d\sin\theta)$, and the two possible points X and X' have coordinates

$$\left(\pm R\sin\left(\theta \pm \phi\right) + \alpha, \pm R\cos\left(\theta \mp \phi\right) + \beta\right),$$

where the upper signs are taken together. In cases 4 and 8, $A_1 = (d\cos\theta, \beta)$ and $A_2 = (0, \beta - d\sin\theta)$, so that the two possible points X and X' have coordinates

$$\left(\pm R\sin\left(\theta \pm \phi\right), \mp R\cos\left(\theta \mp \phi\right) + \beta\right),$$

where the upper signs are taken together.

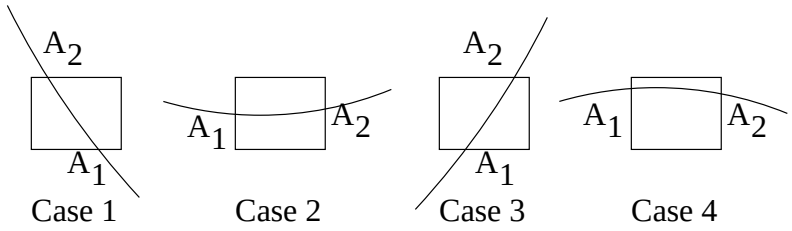
In all of cases 3, 4, 7 and 8, we differentiate with respect to θ to obtain the tangent vector. The tangent vector in cases 3 and 7 is the same as that of (7.6) in cases 1 and 5, so the radius of curvature for the part of the contour in cases 3 and 7 will be approximately R. The tangent vector in cases 4 and 8

differs only by sign changes from the other cases, so this part of the contour again has radius of curvature approximately R. Thus in all eight corner cut cases we have $\rho \simeq R$, and $\mathrm{d}\rho/\,\mathrm{d}\psi$ is $O(R)$. □

7.3 Arcs cutting opposite sides of the rectangle

We now consider the cases of side cuts. There are four types of side cut when we count the orientation of the domain boundary, shown in Figure 7.4. The only difference between side cuts 1 and 3, and side cuts 2 and 4, is whether the line segment A_1A_2 has positive or negative gradient.

Figure 7.4: Side cuts



Lemma 7.2. *The contour lines formed by arcs cutting opposite sides of the rectangle have radius of curvature ρ approximately R. Also in all side cut cases we find that* $\mathrm{d}\rho/\,\mathrm{d}\psi$ *is* $O(R)$.

Proof We consider side cuts 1 and 3 together, setting $0 < k < \alpha$ and $0 < \theta < \pi/2$. In side cut 1, the line A_1A_2 has negative gradient with $A_1 = (k + d\cos\theta, 0)$, $A_2 = (k, \beta)$. In side cut 3, the line A_1A_2 has positive gradient with $A_1 = (k, 0)$, $A_2 = (k + d\cos\theta, \beta)$. The method used to find the points X and X' is the same as that used for the corner cut cases, and we find that in side cut 1, the two possible points X and X' have coordinates

$$\left(\pm R\sin(\theta \pm \phi) + k, \pm R\cos\phi\cos\theta + \frac{\beta}{2}\right),$$

and in side cut 3, X and X' have coordinates

$$\left(\pm R\sin(\theta \pm \phi) + k, \mp R\cos\phi\cos\theta + \frac{\beta}{2}\right),$$

where in both cases the upper signs are taken together.

To show that the radius of curvature for this part of the contour is approximately R, we differentiate with respect to θ to obtain the tangent vectors. The tangent vector in case 1 is

$$\left(\frac{\mathrm{d}x}{\mathrm{d}\theta}, \frac{\mathrm{d}y}{\mathrm{d}\theta}\right) = (\pm R\cos(\theta \pm \phi), \mp R\cos\phi\sin\theta)\,,$$

and the tangent vector in case 3 is

$$\left(\frac{\mathrm{d}x}{\mathrm{d}\theta}, \frac{\mathrm{d}y}{\mathrm{d}\theta}\right) = (\pm R\cos(\theta \pm \phi), \pm R\cos\phi\sin\theta)\,,$$

with upper signs taken together in both cases. From the tangent vectors we obtain

$$\left|\frac{\mathrm{d}s}{\mathrm{d}\theta}\right| = R\left(1 - \sin^2\phi\cos^2\theta \mp \frac{1}{2}\sin 2\phi\sin 2\theta\right)^{1/2}. \tag{7.16}$$

We find that

$$\tan\psi = \mp\frac{\cos\phi\sin\theta}{\cos(\theta \pm \phi)},$$

where $\tan\psi$ is negative in case 1 and positive in case 3. For case 1, we use the identity of (7.9) to find $\tan(\psi + \theta) = f$, where

$$f = \mp\frac{\sin\phi\sin^2\theta}{\cos\phi \mp 1/2\sin\phi\sin 2\theta},$$

so that

$$\psi = -\theta + \tan^{-1} f.$$

For case 3, $\tan\psi$ is the same as in case 1 but with opposite sign. This means that ψ in case 3 is the negative of the ψ obtained in case 1 (possibly differing by a factor of $n\pi$, for integer n) and thus for case 3, the principal value of ψ is $\theta - \tan^{-1} f$.

We now choose to use the case 1 version of ψ with negative f to obtain

$$\frac{\mathrm{d}\psi}{\mathrm{d}\theta} = \frac{\sin^2\phi\sin^2\theta - 1/2\sin 2\phi\sin 2\theta}{1 - \sin^2\phi\cos^2\theta - 1/2\sin 2\phi\sin 2\theta}. \tag{7.17}$$

We obtain the radius of curvature ρ from the results of (7.16) and (7.17),

$$\rho = \frac{R\left(1 - \sin^2\phi\cos^2\theta - 1/2\sin 2\phi\sin 2\theta\right)^{3/2}}{\sin^2\phi\sin^2\theta - 1/2\sin 2\phi\sin 2\theta}.$$

We approximate the radius of curvature as R, using the methods of (7.13).

Again we must establish that the derivative of ρ with respect to ψ is continuous with order of magnitude $O(R)$ or smaller. We already know the derivative of ψ with respect to θ, given in (7.17). We need to calculate the derivative of ρ with respect to θ. To make this calculation more accessible, let

$$\rho = R\frac{b^{3/2}}{c},$$

where

$$b = b(\theta) = 1 - \sin^2\phi\cos^2\theta - 1/2\sin 2\phi\sin 2\theta$$

and

$$c = c(\theta) = \sin^2\phi\sin^2\theta - 1/2\sin 2\phi\sin 2\theta.$$

Then

$$\frac{\mathrm{d}\rho}{\mathrm{d}\theta} = \frac{Rc^{1/2}b'}{b^2}\left(\frac{3}{2}b - c\right), \tag{7.18}$$

where b' is the derivative of b with respect to θ,

$$b' = \sin^2\phi\sin 2\theta - \sin 2\phi\cos 2\theta.$$

We can also express the derivative of ψ with respect to θ in terms of b and c,

$$\frac{\mathrm{d}\psi}{\mathrm{d}\theta} = \frac{b}{c}. \tag{7.19}$$

We use (7.18) and (7.19) and the chain rule to get

$$\frac{\mathrm{d}\rho}{\mathrm{d}\psi} = \frac{Rc^{3/2}b'}{b^3}\left(\frac{3}{2}b - c\right).$$

This is continuous except where $b^3 = 0$, which corresponds to $\theta = 0$ and/or $\theta = \pi/2$. Since we defined $0 < \theta < \pi/2$, the denominator b^3 will be non-zero. The order of magnitude of this derivative is at most R. Calculations and estimates for the remaining cases of side cuts 1 and 3 differ only by sign changes, so that the radius of curvature in all of the cases of side cuts 1 and 3 is approximately R, and $\mathrm{d}\rho/\,\mathrm{d}\psi$ is $O(R)$.

We now consider side cuts 2 and 4, where we set $0 < h < \beta$ and $0 < \theta < \pi/2$. In side cut 2, $A_1 = (0, h + d\sin\theta)$ and $A_2 = (\alpha, h)$, where the line A_1A_2 has negative gradient. In side cut 4, $A_1 = (0, h)$ and $A_2 = (\alpha, h + d\sin\theta)$, where the line A_1A_2 has positive gradient. We find in side cut 2, that the

two points X and X' have coordinates

$$\left(\pm R\cos\phi\cos\theta+\frac{\alpha}{2},R\left(\sin\phi\pm\cos\phi\right)\sin\theta+h\right),$$

and in side cut 4, the two points X and X' have coordinates

$$(x,y)=\left(\pm R\cos\phi\cos\theta+\frac{\alpha}{2},R\left(\sin\phi\mp\cos\phi\right)\sin\theta+h\right),$$

where in all cases the upper signs are taken together.

We differentiate with respect to θ to obtain the tangent vector of side cut 2,

$$\left(\mp R\cos\phi\sin\theta,R\left(\sin\phi\pm\cos\phi\right)\cos\theta\right),$$

and the tangent vector of side cut 4,

$$\left(\mp R\cos\phi\sin\theta,R\left(\sin\phi\mp\cos\phi\right)\cos\theta\right).$$

We use the tangent vectors to find $\mathrm{d}s/\,\mathrm{d}\theta$. For side cut 2

$$\frac{\mathrm{d}s}{\mathrm{d}\theta}=R\left(1-\sin^2\phi\sin^2\theta\pm\sin 2\phi\cos^2\theta\right)^{1/2},$$

and for side cut 4,

$$\frac{\mathrm{d}s}{\mathrm{d}\theta}=R\left(1-\sin^2\phi\sin^2\theta\mp\sin 2\phi\cos^2\theta\right)^{1/2}.$$

We let $t=1-\sin^2\phi\sin^2\theta+\sin 2\phi\cos^2\theta$, and we consider side cut 2 with $\mathrm{d}s/\,\mathrm{d}\theta=Rt^{1/2}$. We find

$$\tan\psi=-\cot\theta(\tan\phi+1),$$

and thus

$$\psi=-\theta+\tan^{-1}\left(\frac{u}{v}\right),$$

with

$$u=-(\cos 2\theta+\tan\phi\cos^2\theta),$$
$$v=\frac{1}{2}(\tan\phi+2)\sin 2\theta.$$

We find the derivative of ψ with respect to θ,

$$\frac{\mathrm{d}\psi}{\mathrm{d}\theta} = \frac{w(\tan\phi + 2) - z}{z}, \tag{7.20}$$

where

$$\begin{aligned} w &= 1 + \frac{1}{2}\tan\phi \sin^2 2\theta + \tan\phi \cos^2\theta \cos 2\theta, \\ z &= 1 + \tan\phi(\tan\phi + 2)\cos^2\theta. \end{aligned}$$

We have $w = vu' - uv'$, where u' is the derivative of u with respect to θ and equals $2v$, and v' is the derivative of v with respect to θ,

$$v' = (\tan\phi + 2)\cos 2\theta.$$

We obtain the radius of curvature from $\mathrm{d}s/\,\mathrm{d}\theta = Rt^{1/2}$ and the result of (7.20),

$$\rho = \frac{Rt^{1/2}}{z}\left(w(\tan\phi + 2) - z\right), \tag{7.21}$$

which is approximately R.

Again we need the derivative of ρ with respect to ψ to be continuous with order of magnitude $O(R)$ or smaller. We already know the derivative of ψ with respect to θ, given in (7.20). We need to calculate the derivative of ρ with respect to θ. We use the form of ρ given in (7.21) and we find that

$$\begin{aligned} \frac{\mathrm{d}\rho}{\mathrm{d}\theta} = {} & \frac{Rt^{1/2}}{z}\frac{\mathrm{d}}{\mathrm{d}\theta}\left(w(\tan\phi + 2)\right) - \frac{Rt^{1/2}}{z}\frac{\mathrm{d}z}{\mathrm{d}\theta} \\ & + \frac{R}{z^2}\left(w(\tan\phi + 2) - z\right)\left(z\frac{\mathrm{d}t^{1/2}}{\mathrm{d}\theta} - t^{1/2}\frac{\mathrm{d}z}{\mathrm{d}\theta}\right). \end{aligned} \tag{7.22}$$

Now

$$\frac{\mathrm{d}z}{\mathrm{d}\theta} = -\tan\phi(\tan\phi + 2)\sin 2\theta = -2v\tan\phi,$$

and

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}\theta}\left(w(\tan\phi + 2)\right) &= (\tan\phi + 2)\frac{\mathrm{d}w}{\mathrm{d}\theta} \\ &= -\tan\phi(\tan\phi + 2)\sin 2\theta \\ &= \frac{\mathrm{d}z}{\mathrm{d}\theta}. \end{aligned}$$

Thus the first part of $\mathrm{d}\rho/\,\mathrm{d}\theta$ in (7.22) cancels, and we are left with

$$\frac{\mathrm{d}\rho}{\mathrm{d}\theta} = \frac{R}{z^2}\left(w(\tan\phi + 2) - z\right)\left(z\frac{\mathrm{d}t^{1/2}}{\mathrm{d}\theta} - t^{1/2}\frac{\mathrm{d}z}{\mathrm{d}\theta}\right).$$

We have already found the derivative of z with respect to θ, and now we find

$$\frac{\mathrm{d}t^{1/2}}{\mathrm{d}\theta} = \frac{1}{2}t^{-1/2}\frac{\mathrm{d}t}{\mathrm{d}\theta} = -\frac{(\sin^2\phi + \sin 2\phi)}{2t^{1/2}}\sin 2\theta.$$

Thus we have

$$\frac{\mathrm{d}\rho}{\mathrm{d}\theta} = \frac{R}{z^2}\left(w(\tan\phi + 2) - z\right)\left(2t^{1/2}v\tan\phi - z\frac{(\sin^2\phi + \sin 2\phi)}{2t^{1/2}}\sin 2\theta\right). \tag{7.23}$$

We use (7.23) and (7.20) and the chain rule to get

$$\frac{\mathrm{d}\rho}{\mathrm{d}\psi} = \frac{R}{z}\left(2t^{1/2}v\tan\phi - z\frac{(\sin^2\phi + \sin 2\phi)}{2t^{1/2}}\sin 2\theta\right)$$

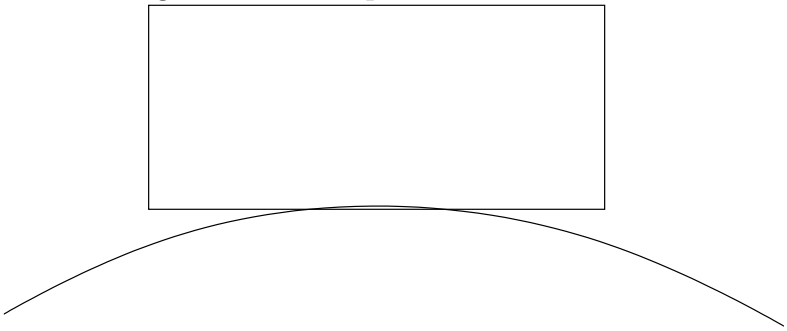
This is continuous except at values of ϕ that correspond to $\theta = 0$ or $\theta = \pi/2$. Since we defined $0 < \theta < \pi/2$, $\mathrm{d}\rho/\,\mathrm{d}\psi$ is continuous everywhere for this case. The derivative $\mathrm{d}\rho/\,\mathrm{d}\psi$ also has order of magnitude of $O(R)$ or smaller. Calculations and estimates for the remaining cases of side cuts 2 and 4 will be similar, so that the radius of curvature in all cases of side cuts 2 and 4 will be approximately R. □

7.4 Rare ways that arcs cut the rectangle

We now consider the rare cases where the straight line between the points A_1 and A_2 has angle of inclination equal to 0 or $\pi/2$. These cases occur when we have opposite side cuts with $A_1 = (k, 0)$ and $A_2 = (k, \beta)$, or with $A_1 = (0, h)$ and $A_2 = (\alpha, h)$, or when we have same-side cuts, with the points A_1 and A_2 lying on the same side of the rectangle.

These short straight segments of lines can be approximated by the arc of the circle of radius R that passes through the points A_1 and A_2 with negligible corrections to the area and number of integer points in $S(t)$. The difference between the straight line and the arc in these cases cannot be illustrated since they are so close together. We attempt to show the difference between the straight line and the arc in Figure 7.5. The radius of the circle to which

Figure 7.5: Example of a same-side cut



the arc of Figure 7.5 belongs is small (about twice the size of the rectangle base), and already the difference is barely discernible.

The last kind of rare case we need to consider are the four-point cuts. Four-point cuts occur where our domain boundary meets the rectangle four times. Four-point cuts can be treated as a combination of corner cuts, demonstrated in Figure 7.6. Since the arcs in corner cuts have radius of curvature approximately R, so will the arcs in four-point cuts.

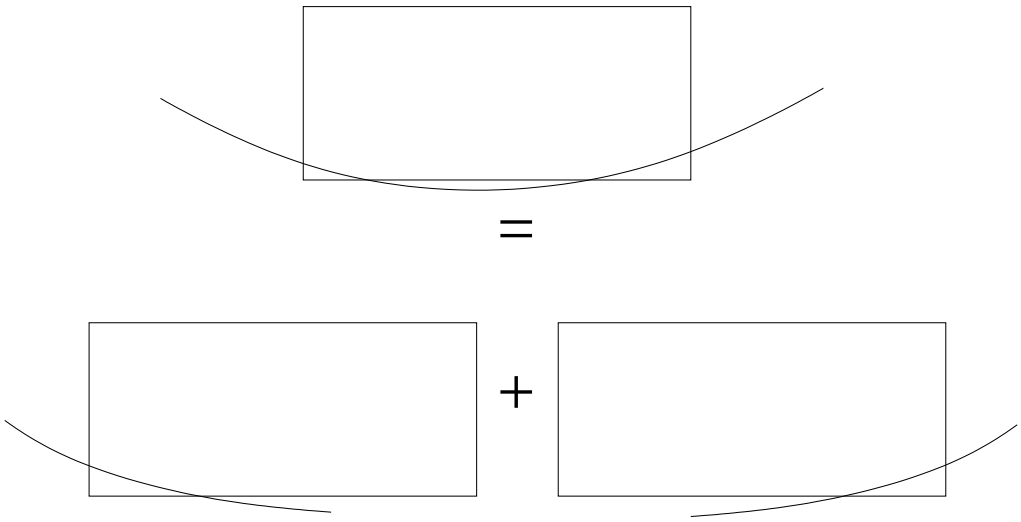


Figure 7.6: Four-point cuts as a combination of arcs

Chapter 8

Analogue of Huxley and Žunić's Lemma and Theorem for intersections of domains

8.1 Number of intersections of domains

Lemma 8.1. *Let L be the total number of intersections within the rectangle $G(\alpha, \beta)$ of ordered pairs of arcs $C(m, n)$ and $C(m', n')$, where (m, n) and (m', n') are distinct critical points in the critical strip $\mathcal{E}$. Then*

$$L = 8\pi R^2 \alpha\beta + O\left(R^{\kappa+1}(\log R)^{\lambda}\right). \tag{8.1}$$

Proof. To calculate asymptotics, we use a continuous model of the discrete integer lattice. We consider the set $E(x, y)$, and the area $e(x, y)$ of the set $E(x, y)$. The area $e(x, y)$ is the shaded region in Figure 7.1, bounded by the circumferences of two equal circles of radius R whose centres are a distance d apart. Thus the area $e(x, y)$ is the sum of the areas of these two equal circles, with twice the area of their intersection subtracted.

As in chapter 7, let $\phi = \phi(x, y)$ be the small angle with $\sin\phi = d/2R$. The common chord of the two circles subtends an angle $\pi - 2\phi$ at the centre of each circle. The area of the intersection of the two circles is calculated using basic trigonometry as $(\pi - 2\phi)R^2 - dR\cos\phi$. The area of the two circles in total is $2\pi R^2$ so we have the area $e(x, y)$,

$$e(x, y) = 2\pi R^2 - 2((\pi - 2\phi)R^2 - dR\cos\phi) = 4\phi R^2 + 2dR\cos\phi.$$

We use the power series expansions of $\cos\phi$ and $\sin\phi$ with the defining identity $\sin\phi = d/2R$ to give our approximations to ϕ and $\cos\phi$,

$$\phi = \frac{d}{2R} + O\left(\frac{d^3}{R^3}\right) = \frac{d}{2R} + O\left(\frac{1}{R^3}\right),$$

and

$$\cos\phi = 1 - \frac{\phi^2}{2} + O\left(\frac{1}{R^4}\right) = 1 - O\left(\frac{1}{R^2}\right),$$

which means that

$$e(x,y) = 4dR + O\left(\frac{1}{R}\right). \tag{8.2}$$

For each critical point (m,n) in $\mathcal{E}$ we want to count the number of arcs $C(m',n')$ that cross $C(m,n)$ once only. By Proposition 6.1, the sum is

$$\sum_{(m,n)\in\mathcal{E}} \big(e(m,n) + O(R^\kappa(\log\ R)^\lambda)\big) = \sum_{(m,n)\in\mathcal{E}} e(m,n)\ +\ O(R^{\kappa+1}(\log R)^\lambda). \tag{8.3}$$

We want to replace the first term in (8.3) by

$$\iint_{\mathcal{E}} e(x,y)\,\mathrm{d}x\,\mathrm{d}y.$$

However, the function $e(x,y)$ is zero on the boundary of the critical strip $\mathcal{E}$, and has partial derivatives of size R, as shown in chapter 7. This means that the integer lattice has too few points to be used for straightforward numerical integration.

Let T be the maximum of $e(x,y)$. For $t \le e(x,y) \le T$, let $S(t)$ be the subset of $\mathcal{E}$ on which $e(x,y) \ge t$. Let $\chi_{S(t)}(x,y)$ be the characteristic function of $S(t)$, which equals 1 if $(x,y) \in S(t)$, and 0 otherwise. We use the Riesz interchange principle [34]. We have

$$e(x,y) = \int_0^T \chi_{S(t)}(x,y)\,\mathrm{d}t.$$

Summing over critical points (m,n), we have

$$\begin{aligned}\sum_{(m,n)\in\mathcal{E}} e(m,n) &= \sum_{(m,n)\in\mathcal{E}} \int_0^T \chi_{S(t)}(m,n)\,\mathrm{d}t \\ &= \int_0^T \sum_{(m,n)\in\mathcal{E}} \chi_{S(t)}(m,n)\,\mathrm{d}t \\ &= \int_0^T \sum_{(m,n)\in S(t)} 1\,\mathrm{d}t \\ &= \int_0^T N(t)\,\mathrm{d}t. \end{aligned} \tag{8.4}$$

The region $S(t)$ is bounded by contour lines of the function $e(x,y)$. The contour lines are the locus of the points (x,y) for which the distance d between the points of intersection $A_1(x,y)$ and $A_2(x,y)$ is fixed. Given $A_1(x,y)$ and $A_2(x,y)$, there are two possible positions for the point (x,y), which we called X and X' in chapter 7. We saw that the critical strip $\mathcal{E}$ is bounded by circular arcs of radius R, and that $S(t)$ is bounded by contour lines whose radius of curvature is approximately R.

Let $f(t)$ be the area of $S(t)$. From Proposition 6.1, we have

$$N(t) = f(t) + O\left(R^{\kappa}(\log R)^{\lambda}\right).$$

We use this in (8.4) to obtain

$$\sum_{(m,n)\in\mathcal{E}} e(m,n) = \int_0^T f(t)\,\mathrm{d}t + O\left(R^{\kappa+1}(\log R)^{\lambda}\right). \tag{8.5}$$

We have used the fact that the maximum value T of $e(x,y)$ is the area of the critical strip $\mathcal{E}$, which is $O(R)$.

When the point (x,y) lies on the boundary of the critical strip $\mathcal{E}$, we have $e(x,y) = 0$. For $t > 0$ the contour lines of $e(x,y)$ bounding $S(t)$ lie completely within the critical strip $\mathcal{E}$. The area t is an increasing function of the distance d. For $d \le \min\{\alpha,\beta\}$, the set $S(t)$ forms a narrower strip within the critical strip $\mathcal{E}$, bounded by contour lines whose radius of curvature is approximately R, which are of the form

$$\left(\pm R\sin\left(\theta \pm \phi\right), \pm R\cos\left(\theta \mp \phi\right)\right), \tag{8.6}$$

where the upper signs are taken together.

For $\min\{\alpha,\beta\} < d \le \sqrt{\alpha^2+\beta^2}$ the set $S(t)$ consists of two disconnected parts. The contour lines have long arcs of the type (8.6) which end at points (x,y) where either $A_1(x,y)$ or $A_2(x,y)$ becomes a vertex of the rectangle $G(\alpha,\beta)$. These curved arcs are joined by line segments equal and parallel to one of the sides of the rectangle.

The set $S(t)$ has the fourfold symmetry of the rectangle $G(\alpha,\beta)$. We consider the 'first quadrant' of the set $S(t)$, where the contour lines are curves (8.6) with gradient increasing (anticlockwise) through negative values from $-\infty$ to 0. These contour lines are parameterised by

$$\left(R\cos\phi\sin\theta+\frac{d}{2}\cos\theta, R\cos\phi\cos\theta+\frac{d}{2}\sin\theta\right),$$

and

$$\left(R\cos\phi\sin\theta-\frac{d}{2}\cos\theta+\alpha, R\cos\phi\cos\theta-\frac{d}{2}\sin\theta+\beta\right),$$

whose polar coordinates (r,Θ) satisfy

$$\Theta=\frac{\pi}{2}-\theta+O\left(\frac{1}{R}\right)$$

with

$$\frac{\mathrm{d}\Theta}{\mathrm{d}\theta}=-1+O\left(\frac{1}{R}\right), \tag{8.7}$$

and

$$r=r_1+O\left(\frac{1}{R}\right),\ r=r_2+O\left(\frac{1}{R}\right)$$

on the lower and upper boundaries respectively (see Appendix 1 for details), where

$$r_1=R+\frac{d}{2}\sin 2\theta,\ r_2=R+\alpha\sin\theta+\beta\cos\theta-\frac{d}{2}\sin 2\theta.$$

We want to find the area using these polar coordinates,

$$\int_0^{\frac{\pi}{2}}\int_{r_1}^{r_2}\mathrm{d}r\,\mathrm{d}\Theta.$$

Using the result of (8.7), this is equivalent to

$$\int_0^{\frac{\pi}{2}}\int_{r_1}^{r_2}\mathrm{d}r\,\mathrm{d}\theta+O\left(\frac{1}{R}\left|\int_0^{\frac{\pi}{2}}\int\mathrm{d}r\,\mathrm{d}\theta\right|\right). \tag{8.8}$$

We begin by estimating the integral of the radial polar coordinate r in the implicit first quadrant,

$$\int_{r_1}^{r_2} r \, \mathrm{d}r = \frac{r_2^2}{2} - \frac{r_1^2}{2},$$

which we estimate as

$$\alpha R \sin\theta + \beta R \cos\theta - dR \sin 2\theta + O(1). \tag{8.9}$$

We use this in the order of magnitude term from (8.8), and integrate with respect to θ between 0 and $\pi/2$, so that the order of magnitude term in (8.8) becomes $O(1)$, and thus

$$\int_0^{\frac{\pi}{2}} \int_{r_1}^{r_2} \mathrm{d}r \, \mathrm{d}\Theta = \int_0^{\frac{\pi}{2}} \int_{r_1}^{r_2} \mathrm{d}r \, \mathrm{d}\theta + O(1)$$

In order to obtain $f(t)$, we multiply the term from (8.9) by 4 and factorise to get $4R(\alpha \sin\theta + \beta \cos\theta - d \sin 2\theta \, \mathrm{d}\theta) + O(1)$. We then express $f(t)$ as an integral of this term with respect to θ between 0 and $\pi/2$,

$$f(t) = 4R \int_0^{\frac{\pi}{2}} (\alpha \sin\theta + \beta \cos\theta - d \sin 2\theta) \, \mathrm{d}\theta + O(1). \tag{8.10}$$

Since the result of (8.2) gives us $t = e(x, y) = 4dR + O(1)$ we have

$$d = \frac{t}{4R} + O\left(\frac{1}{R}\right).$$

We use the substitution $l = t/4R$, giving $d = l + O(1/R)$, so that the integral in (8.5) is

$$\int_0^T f(t) \, \mathrm{d}t = 4R \int_0^L f(4Rl) \, \mathrm{d}l. \tag{8.11}$$

Consequently, the integral in (8.11) combines with (8.10) to give

$$16R^2 \int_0^{\pi/2} \int_0^L (\alpha \sin\theta + \beta \cos\theta - l \sin 2\theta) \, \mathrm{d}l \, \mathrm{d}\theta + O(R). \tag{8.12}$$

There are two cases we need to consider, $0 \leq \theta \leq \tan^{-1}(\beta/\alpha)$ and $\tan^{-1}(\beta/\alpha) \leq \theta \leq \pi/2$. For $\theta \leq \tan^{-1}(\beta/\alpha)$, we have $l \leq \alpha \sec\theta$, and for $\theta \geq \tan^{-1}(\beta/\alpha)$, we have $l \leq \beta \operatorname{cosec}\theta$. The first case has $L = \alpha \sec\theta$,

and

$$\begin{aligned}
&\int_0^{\alpha\sec\theta} (\alpha\sin\theta + \beta\cos\theta - l\sin 2\theta)\,\mathrm{d}l \\
&= \left[\alpha l\sin\theta + \beta l\cos\theta - \frac{l^2}{2}\sin 2\theta\right]_0^{\alpha\sec\theta} \\
&= \alpha^2\tan\theta + \alpha\beta - \alpha^2\tan\theta \\
&= \alpha\beta.
\end{aligned}$$

The second case has $L = \beta\operatorname{cosec}\theta$, and

$$\begin{aligned}
&\int_0^{\beta\operatorname{cosec}\theta} \alpha\sin\theta + \beta\cos\theta - l\sin 2\theta\,\mathrm{d}l \\
&= \left[\alpha l\sin\theta + \beta l\cos\theta - \frac{l^2}{2}\sin 2\theta\right]_0^{\beta\operatorname{cosec}\theta} \\
&= \alpha\beta + \beta^2\cot\theta - \beta^2\cot\theta \\
&= \alpha\beta.
\end{aligned}$$

Hence

$$\begin{aligned}
&16R^2\int_0^{\tan^{-1}(\beta/\alpha)}\int_0^{\alpha\sec\theta} \alpha\sin\theta + \beta\cos\theta - l\sin 2\theta\,\mathrm{d}l\,\mathrm{d}\theta \\
=&16R^2\int_0^{\tan^{-1}(\beta/\alpha)} \alpha\beta\,\mathrm{d}\theta,
\end{aligned}$$

and

$$\begin{aligned}
&16R^2\int_{\tan^{-1}(\beta/\alpha)}^{\pi/2}\int_0^{\beta\operatorname{cosec}\theta} \alpha\sin\theta + \beta\cos\theta - l\sin 2\theta\,\mathrm{d}l\,\mathrm{d}\theta \\
=&16R^2\int_{\tan^{-1}(\beta/\alpha)}^{\pi/2} \alpha\beta\,\mathrm{d}\theta,
\end{aligned}$$

so that (8.12) becomes

$$\begin{aligned}
&16R^2\int_0^{\tan^{-1}(\beta/\alpha)} \alpha\beta\,\mathrm{d}\theta + 16R^2\int_{\tan^{-1}(\beta/\alpha)}^{\pi/2} \alpha\beta\,\mathrm{d}\theta + O(R) \\
=&16R^2\int_0^{\pi/2} \alpha\beta\,\mathrm{d}\theta + O(R) \\
=&8\pi R^2\alpha\beta + O(R).
\end{aligned}$$

This calculation evaluates the integral in (8.5), and gives the result of (8.1), thereby completing our proof. □

The result sketched by Huxley and Žunić in [23] was the case $\alpha = \beta = 1$, when the rectangle is the whole unit square.

8.2 Number of regions of rectangles given by domain boundaries

Theorem 7. *The number of domains which meet the rectangle $G(\alpha, \beta)$ is*

$$4\pi R^2 \alpha\beta + O\left(R^{\kappa+1}(\log R)^{\lambda}\right),$$

where $\kappa = 131/208$ and $\lambda = 18627/8320$.

Proof. To estimate the number of regions of the rectangle $G(\alpha, \beta)$ made by the arcs $C(m, n)$, we move from counting domains to counting vertices of domains. For all but a discrete sequence of radii R, any circle of radius R satisfies the Triangle Condition, so that the circle passes through at most two integer points, and hence domains meet in fours, with no multiple intersections of domain boundaries.

We form a graph from the perimeter of the rectangle and the arcs of the circles that form domain boundaries within the rectangle, both directed anticlockwise. In Section 6.2 we saw that $O(R)$ domain boundaries enter or leave the rectangle. The vertices are where domain boundaries meet one another, or meet the perimeter of the rectangle.

When the Triangle Condition, stated in Section 5.3, holds, then vertices inside the rectangle have four edges, two starting and two ending at that vertex. Vertices on the perimeter of the rectangle have three or perhaps four edges.

When the Triangle Condition fails for the radius R, there is an extra complication. The point P is called a bad point if three or more arcs $C(m, n)$ meet at the point P. This means that there exist k (≥ 3) critical points $(m_1, n_1), \ldots, (m_k, n_k)$ on the circle $C(P)$. The upper bound for k is $k \leq \Delta$ where Δ is the maximum, taken over positive integers $n \leq 8D = 32R^2(2R + 1)^2$, of the number of ways of writing n as a sum of two squares of integers, so that as in [13], $\Delta = O(R^{\eta})$ for any $\eta > 0$. Therefore, for any bad point P

in the rectangle $G(\alpha, \beta)$, the number of arcs $C(m, n)$ through P is bounded above by $O\left(R^{\eta}\right)$.

Lemma 3.2 of [23] assures us that there are $O\left(R^{\epsilon}\right)$ bad points P located in the whole unit square, for any $\epsilon > 0$. Hence there are $O\left(R^{\epsilon}\right)$ bad points P in the rectangle $G(\alpha, \beta)$.

Let F be the number of domains that meet the rectangle $G(\alpha, \beta)$. Let E be the number of edges in the graph defined above, and let V be the number of vertices. By Euler's formula $(F + 1) + V = E + 2$.

First we suppose that the Triangle Condition holds. Lemma 8.1 counts ordered pairs of arcs, so there are $L/2$ vertices at which two arcs $C(m, n)$ and $C(m', n')$ meet, and $O(R)$ other vertices on the perimeter. There are four edges at each of these vertices, even if it is one of the $O(R)$ vertices on the perimeter. Hence

$$V = \frac{L}{2} + O(R), \;\; E = L + O(R),$$

and so

$$F = \frac{L}{2} + O(R).$$

When the Triangle Condition fails for the radius R, then there are $O(R^{\epsilon})$ bad vertices, each counted with multiplicity at most $\Delta^2 = O(R^{2\eta})$ in L. Hence

$$V = \frac{L}{2} + O(R) - O\left(R^{\epsilon+2\eta}\right)$$
$$E = \frac{L}{2} + O(R) - O\left(R^{\epsilon+2\eta}\right).$$

When ϵ and η are taken sufficiently small, we still obtain

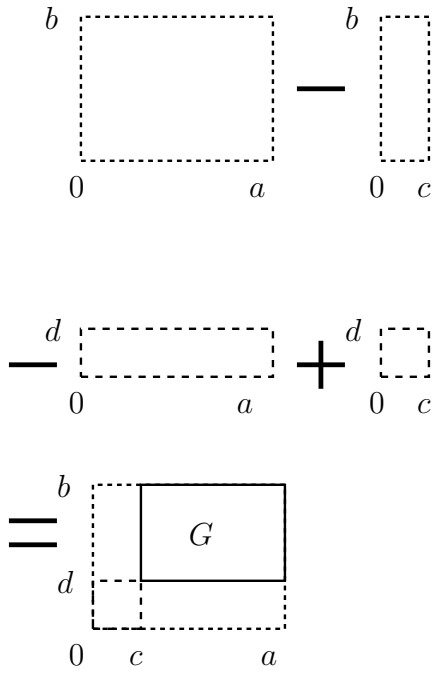
$$F = \frac{L}{2} + O(R).$$

Hence by (8.1), whether the Triangle Condition holds for the radius R or not, we have

$$F = 4\pi R^2 \alpha\beta + O\left(R^{\kappa+1}(\log R)^{\lambda}\right). \tag{8.13}$$

Usually each of these F regions corresponds to a different domain. We recall from Section 5.3 that a domain can become disconnected as the radius R increases when two opposite boundary arcs, concave with respect to the domain, expand to touch and cross. Lemma 2.4 of [25] on disconnected

Figure 8.1: Reproduction of Figure 5.4



domains tells us that this extremely unusual case occurs at most $O(R)$ times. So the number of distinct domains which meet the rectangle $G(\alpha, \beta)$ is $F - O(R)$, and the extra error term of size $O(R)$ is absorbed by the existing error term in (8.13). □

8.3 Uniform distribution modulo the integer lattice

The number of regions of the rectangle $G(\alpha, \beta)$ formed by domain boundaries is $4\pi R^2 \alpha\beta$ up to an error term, which will be the same for the rectangle $G(\beta, \alpha)$ by the commutativity of multiplication, so that the order of α and β is unimportant in our result of Theorem 7.

In Chapter 5 we introduced the general rectangle, G, of Figure 5.3. The general rectangle G did not have the origin as a corner, but its sides were parallel to the axes. The number of domains in G could be found by considering rectangles with the origin as a corner and adding and subtracting the number of domains in these rectangles, as demonstrated in Figure 5.4, which we reproduce here for reference.

We let the dimensions of G be $a - c = \alpha$ and $b - d = \beta$. Then, ignoring error terms for ease of calculation, the number of regions of the rectangle G formed by domain boundaries will be

$$\begin{aligned} & 4\pi R^2 ab - 4\pi R^2 bc - 4\pi R^2 ad + 4\pi R^2 cd \\ =& 4\pi R^2 (ab - bc - ad - cd) \\ =& 4\pi R^2 (a - c)(b - d) \\ =& 4\pi R^2 \alpha\beta, \end{aligned}$$

showing that our result for the rectangle $G(\alpha, \beta)$ is independent of its position within the unit square, as long as its sides remain parallel to the axes.

Since the position of the rectangle $G(\alpha, \beta)$ within the unit square does not matter, and nor does the order of α and β, there will be the same number of domains within the rectangle regardless of the location of the rectangle, and thus the domains are uniformly distributed modulo the integer lattice.

8.4 Sketching an alternative approach

Uniform distribution is usually proved indirectly using Weyl's criterion. In 2 dimensions, Weyl's criterion states that a set of points (x_μ, y_μ), where the index μ runs through some infinite sequence, tends to uniform distribution when the exponential sums

$$S(g, h) = \sum_{\mu} e\left(g x_\mu + h y_\mu\right), \tag{8.14}$$

taken over $\mu \in Q$, a finite initial segment of the sequence, have smaller order of magnitude than the number of terms in Q, as the initial segment Q tends to infinity.

We have a set of domains rather than a set of points, but we have vertices in the domain diagram which correspond to points. Thus a proof using Weyl's Criterion would show that this set of points, the vertices of the domain diagram, is uniformly distributed. We would then be able to deduce the uniform distribution of the domains themselves.

Kolountzakis [19] made the observation that the intersections of ordered pairs of arcs $C(m_1, n_1)$ and $C(m_2, n_2)$ are parameterised by the integer vectors $(m_1 - m_2, n_1 - n_2) = (m, n)$ say. The point U of intersection corresponds

to two points V_1, V_2 on the circle $x^2 + y^2 = R^2$ with $\overrightarrow{V_1V_2} = (m, n)$. The points V_1 and V_2 reduce to the same point $V(m, n) = \big(x_{(m,n)}, y_{(m,n)}\big)$ in the unit square modulo the integer lattice. We would replace the index μ with (x, y) in 8.14.

A quantitative version of Weyl's criterion for uniform distribution module one is given by the inequality of Erdős and Turàn [6]. This gives an estimate for the discrepancy of a sequence of real numbers in terms of exponential sums. Koksma extended the Erdős-Turàn inequality to two or more dimensions, providing an upper bound for the discrepancy of large point sets, and the result is known as the Erdős-Turàn-Koksma inequality [28].

The Erdős-Turàn-Koksma Inequality. Let $x_1, \ldots, x_N$ be points in I^s, the s-dimensional unit cube, and H be an arbitrary positive integer. Then the discrepancy $D_N^*(x_1, \ldots, x_N)$ satisfies

$$D_N^*(x_1, \ldots, x_N) \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \sum_{0<\|h\|_\infty \leq H} \frac{1}{r(h)} \left| \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i \langle h, x_n \rangle} \right| \right),$$

where

$$r(h) = \prod_{i=1}^{s} \max\{1, |h_i|\}$$

for $h = (h_1, \ldots, h_s) \in \mathbb{Z}^s$.

The idea is to use the row-of-teeth function $\rho(t) = [t] - t + 1/2$, where $[t]$ is the greatest integer n such that $n \leq t$, to pick out a condition $0 \leq x \leq \alpha$. The function $\rho(t)$ can be approximated from above and below by finite Fourier series. We sum the finite Fourier series term-by-term to get the sum over intersection points $(x, y) = \big(x_{(m,n)}, y_{(m,n)}\big)$.

The parameterising points lie in a circle of radius $2R$. The circle of radius $2R$ will be broken up into smaller regions. We have a two dimensional Fourier series with two indices, so that Fourier coefficients are indexed by the integer vectors in the plane. We want to divide the plane into regions and use different methods in different regions. However, there is not a finite number of regions so we will need to choose a cut off point. Regions will get smaller and smaller approaching the cut off point, but the regions have to form convex shapes. This is a geometrical complication. Also there is no clear choice of cut off point for the regions, and indeed no clear choice of regions, so this division of the exponential sums and change in coordinates is more

complicated than the original method and will not be simpler. With much hard work Huxley believes it should be possible to obtain some cancellation in the outer sum over m, as well as in the inner sum over n.

In our approach we have counted integer points in regions of the critical strip $\mathcal{E}$ bounded by contour lines. At the very outset we count the number of integer points (m, n) in the critical strip $\mathcal{E}$, a region composed of two crescents, formed by the arcs of two circles. At this stage we only need an upper bound of the right order of magnitude, which we have from using the "area plus order of perimeter" estimate, $AR^2 + O(R)$.

We use a continuous variable of integration l to parameterise the contour lines, giving a continuous family of lattice point problems. There are results in the literature where a slightly better bound is found on average [14, 17] for a family of lattice point problems. Our family of contour lines is not, however, covered by these results, and it is not immediately obvious how to proceed.

Thus both our approach and the Weyl criterion approach offer some possibility for improving the error estimate in Theorem 7, and thus obtaining a finer uniform distribution result. Such improvements lie beyond the scope of the current PhD project.

Bibliography

[1] S. Bayer. *Lattice Points in Plane Areas*. Unpublished undergraduate project, 2006.

[2] M. Beck and S. Robins. *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*. Springer, 2007.

[3] E. Bombieri and H. Iwaniec. Some mean-value theorems for exponential sums. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 13(3):473–486, 1986.

[4] L. Comtet. *Advanced Combinatorics: The Art of Finite and Infinite Expansions*. Dordrecht, 1974.

[5] H. Davenport, P. Erdős, and W.J. LeVeque. On Weyl's Criterion for uniform distribution. *Michigan Math. J.*, 10:311–314, 1963.

[6] P. Erdős and P. Turán. On a problem in the theory of uniform distribution I. *Indag. Math*, 10:370–378, 1948.

[7] Euclid. *The elements of Euclid edited by Isaac Todhunter with an introduction by Sir Thomas L. Heath*. Everyman's Library: Dent, 1933.

[8] C.F. Gauss. *De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem*. Werke, Zweiter Band, Königlichen Gesellschaft der Wiss. Göttingen, 1876.

[9] C.F. Gauss. *Disquisitiones Arithmeticae (translated by Arthur A. Clarke)*. Yale University Press, 1966.

[10] S.W. Graham and G. Kolesnik. *Van der Corput's Method of Exponential Sums*. LMS Notes, Cambridge University Press, 1991.

[11] R.K. Guy. *Unsolved Problems in Number Theory*. Springer, 3rd edition, 2004.

[12] G.H. Hardy, J.E. Littlewood, and G. Pólya. *Inequalities*. Cambridge University Press, 2nd edition, 1952.

[13] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, 5th edition, 1979.

[14] M.N. Huxley. Exponential Sums and Lattice Points II. *Proc. Lond. Math. Soc. (3)*, 66(2):279–301, 1993.

[15] M.N. Huxley. *Area, Lattice Points, and Exponential Sums*. Clarendon Press, Oxford, 1996.

[16] M.N. Huxley. The Integer Points Close to a Curve II. In *Analytic number theory: proceedings of a conference in honor of Heini Halberstam*, volume 2, pages 487–516. Birkhäuser, 1996.

[17] M.N. Huxley. Exponential sums and lattice points III. *Proc. Lond. Math. Soc. (3)*, 87(3):591–609, 2003.

[18] M.N. Huxley. Exponential sums and the Riemann zeta function V. *Proc. Lond. Math. Soc. (3)*, 90(1):1–41, 2005.

[19] M.N. Huxley, M. Kolountzakis, and J. Žunić. The Number of Configurations in Lattice Point Counting III. *In preparation*.

[20] M.N. Huxley and S.V. Konyagin. Cyclic Polygons of Integer Points. *Acta Arith.*, 138(2):109–136, 2009.

[21] M.N. Huxley and N. Watt. The Number of Ideals in a Quadratic Field II. *Israel J. Math.*, 120(part A):125–153, 2000.

[22] M.N. Huxley and J. Žunić. The Number of Configurations in Lattice Point Counting II. *Submitted*.

[23] M.N. Huxley and J. Žunić. Different Digitisations of Displaced Discs. *Found. Comput. Math.*, 6(2):255–268, 2006.

[24] M.N. Huxley and J. Žunić. The Number of N-Point Digital Discs. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(1):159–161, 2007.

[25] M.N. Huxley and J. Žunić. The Number of Configurations in Lattice Point Counting I. *Forum Math.*, 22(1):127–152, 2010.

[26] H. Iwaniec and C.J. Mozzochi. On the divisor and circle problems. *J. Number Theory*, 29(1):60–93, 1988.

[27] D.G. Kendall. On the number of lattice points inside a random oval. *Quart. J. Math. Oxford Ser.*, 19:1–26, 1948.

[28] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. Wiley, New York, 1974.

[29] D.S. Mitrinović. *Analytic Inequalities*. Springer-Verlag, Berlin, 1970.

[30] H.L. Montgomery and R.C. Vaughan. *Cambridge studies in advanced mathematics 97: Multiplicative Number Theory I. Classical Theory*. Cambridge University Press, 2007.

[31] A.S. Ramanujan. Some formulae in the analytic theory of numbers. *Messenger Math.*, 45:81–84, 1916.

[32] A.S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proc. Lond. Math. Soc. (2)*, 17(1):75–115, 1918.

[33] A.S. Ramanujan. *Collected Papers of Aiyangar Srinivasa Ramanujan*. Cambridge University Press, 1927.

[34] M. Riesz, L. Gårding, and L. Hörmander. *Collected Papers of Marcel Riesz*. Springer-Verlag, 1988.

[35] A. Schinzel. Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières. *Enseign. Math. (2)*, IV(1):71–72, 1958.

[36] W. Sierpiński. O pewnym zagadnieniu z rachunku funkcji asymptotycznych. *Prace Mat.-Fiz.*, 17:77–118, 1906.

[37] E.C. Titchmarsh. *The Theory of the Riemann Zeta-function*. Oxford University Press, 2nd edition, 1986.

[38] J.G. van der Corput. *Over roosterpunten in het platte vlak (de beteekenis van de methoden van Voronoï en Pfeiffer)*. Groningen, Noordhoff, 1919.

[39] G. Voronoï. Sur un problème du calcul des fonctions asymptotiques. *J. Reine Angew. Math.*, 126:241–282, 1903.

[40] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

[41] E.T. Whittaker and G.N. Watson. *A Course of Modern Analysis*. Cambridge University Press, 2002.

[42] B.M. Wilson. Proofs of some formulae enunciated by Ramanujan. *Proc. Lond. Math. Soc. (2)*, 21:235–255, 1922.

Appendix A

Polar coordinate calculations

In chapter 8 we have contour lines parameterised by

$$\left(R\cos\phi\sin\theta+\frac{d}{2}\cos\theta, R\cos\phi\cos\theta+\frac{d}{2}\sin\theta\right), \tag{A.1}$$

and

$$\left(R\cos\phi\sin\theta-\frac{d}{2}\cos\theta+\alpha, R\cos\phi\cos\theta-\frac{d}{2}\sin\theta+\beta\right), \tag{A.2}$$

as θ varies, where ϕ is fixed, $d=2R\sin\phi$ and $0<\alpha\leq 1$, $0<\beta\leq 1$. We give here the details of how we found the polar coordinates (r,Θ) of these contour lines, and how we estimated the area between the contour lines.

A.1 Finding the polar coordinates

We found in chapter 8 that the first set of polar coordinates have

$$r=R+\frac{d}{2}\sin 2\theta+O\left(\frac{1}{R}\right), \quad \Theta=\frac{\pi}{2}-\theta+O\left(\frac{1}{R}\right).$$

From (A.1) we have

$$\begin{aligned} r^2 &= \left(R\cos\phi\sin\theta+\frac{d}{2}\cos\theta\right)^2+\left(R\cos\phi\cos\theta+\frac{d}{2}\sin\theta\right)^2 \\ &= R^2\cos^2\phi+dR\cos\phi\sin 2\theta+\frac{d^2}{4} \\ &= \left(R\cos\phi+\frac{d}{2}\sin 2\theta\right)^2+\frac{d^2}{4}\cos^2 2\theta. \end{aligned}$$

Thus

$$r = \left(R\cos\phi + \frac{d}{2}\sin 2\theta \right) \left(1 + O\left(\frac{d^2}{R^2} \right) \right).$$

Now we use the power series expansion of $\cos\phi$ with the defining identity $\sin\phi = d/2R$ to give an approximation to $\cos\phi$,

$$\cos\phi = 1 - \frac{\phi^2}{2} + O\left(\frac{1}{R^4} \right) = 1 - O\left(\frac{1}{R^2} \right),$$

so that

$$\begin{aligned} r &= \left(R\left(1 - O\left(\frac{1}{R^2} \right) \right) + \frac{d}{2}\sin 2\theta \right) \left(1 + O\left(\frac{d^2}{R^2} \right) \right) \\ &= \left(R + \frac{d}{2}\sin 2\theta - O\left(\frac{1}{R^2} \right) \right) \left(1 + O\left(\frac{d^2}{R^2} \right) \right) \\ &= R + \frac{d}{2}\sin 2\theta + O\left(\frac{1}{R^2} \right). \end{aligned}$$

We then consider $\tan\Theta$, using $d = 2R\sin\phi$ to get

$$\begin{aligned} \tan\Theta &= \frac{R\cos\phi\cos\theta + R\sin\phi\sin\theta}{R\cos\phi\sin\theta + R\sin\phi\cos\theta} \\ &= \frac{\cos\phi\sin\left(\pi/2 - \theta\right) + \sin\phi\cos\left(\pi/2 - \theta\right)}{\cos\phi\cos\left(\pi/2 - \theta\right) + \sin\phi\sin\left(\pi/2 - \theta\right)} \\ &= \frac{\sin\left(\pi/2 - \theta + \phi\right)}{\cos\left(\pi/2 - \theta - \phi\right)}. \end{aligned}$$

We use the power series expansion of $\sin\phi$ with the defining identity $\sin\phi = d/2R$ to give an approximations to ϕ,

$$\phi = \frac{d}{2R} + O\left(\frac{d^3}{R^3} \right) = O\left(\frac{1}{R} \right).$$

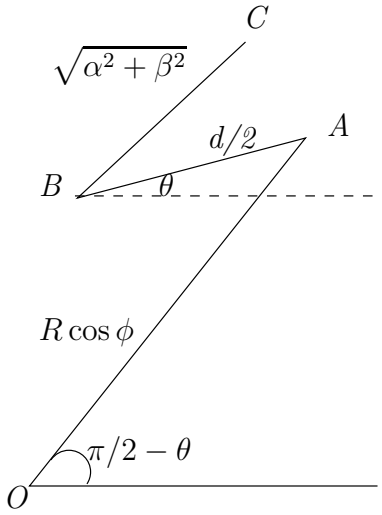
This means we have

$$\tan\Theta = \tan\left(\frac{\pi}{2} - \theta + O\left(\frac{1}{R} \right) \right).$$

For θ in the first quadrant we have

$$\Theta = \frac{\pi}{2} - \theta + O\left(\frac{1}{R} \right).$$

Figure A.1: Polar coordinate diagram of vector sums



The second set of polar coordinates we found were

$$r = R + \alpha\sin\theta + \beta\cos\theta - \frac{d}{2}\sin 2\theta + O\left(\frac{1}{R}\right) \quad \Theta = \frac{\pi}{2} - \theta + O\left(\frac{1}{R}\right).$$

We rewrite (A.2) as a vector sum,

$$\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{AB} + \overrightarrow{BC} = R\cos\phi(\sin\theta, \cos\theta) - \frac{d}{2}(\cos\theta, \sin\theta) + (\alpha, \beta),$$

and we depict this in Figure A.1. The magnitude of the vector $\overrightarrow{OC}$ gives the polar coordinate, r, and the direction of the vector $\overrightarrow{OC}$ gives the angular polar coordinate, Θ. The distance of C from the line OA, with the line OA extended through A if necessary, is Y, where

$$Y \leq AB + BC = \frac{d}{2} + \sqrt{\alpha^2+\beta^2} \leq \frac{3}{2}\sqrt{\alpha^2+\beta^2} \leq \frac{3}{2}\sqrt{2} = O(1).$$

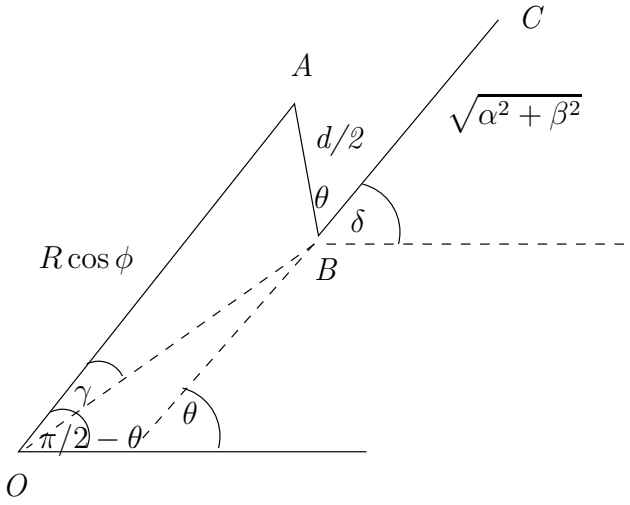
The component of $\overrightarrow{OC}$ in the direction of OA is

$$OA - AB\cos\widehat{OAB} + BC\cos\gamma,$$

where γ is the angle between OA and BC (Figure A.2). The angle $\widehat{OAB} = 2\theta - \pi/2$ so that

$$\cos\widehat{OAB} = \cos(2\theta - \pi/2) = \cos(\pi/2 - 2\theta) = \sin(2\theta).$$

Figure A.2: Diagram of vectors, angles and components



The line BC has gradient $\beta/\alpha = \tan\delta$, so that γ, the angle between OA and BC is $\pi/2 - \theta - \delta$, and

$$\cos\gamma = \cos(\pi/2 - \theta - \delta) = \sin(\theta + \delta).$$

Thus the component of $\overrightarrow{OC}$ in the direction of OA is

$$\begin{aligned} X &= |OA| - |AB|\sin 2\theta + |BC|\sin(\theta+\delta) \\ &= R\cos\phi - \frac{d}{2}\sin 2\theta + \sqrt{\alpha^2+\beta^2}\sin(\theta+\delta) \\ &= R - \frac{d}{2}\sin 2\theta + \sqrt{\alpha^2+\beta^2}\sin(\theta+\delta) - O\left(\frac{1}{R}\right). \end{aligned}$$

We expand the $\sqrt{\alpha^2+\beta^2}\,\sin(\theta+\delta)$ term,

$$\sqrt{\alpha^2+\beta^2}\,\sin(\theta+\delta) = \sqrt{\alpha^2+\beta^2}\,(\sin\theta\cos\delta + \cos\theta\sin\delta).$$

Now $\tan\delta = \beta/\alpha$, which means

$$\sin\delta = \frac{\beta}{\sqrt{\alpha^2+\beta^2}},\ \cos\delta = \frac{\alpha}{\sqrt{\alpha^2+\beta^2}},$$

and thus

$$\sqrt{\alpha^2+\beta^2}\,\sin(\theta+\delta) = \alpha\sin\theta + \beta\cos\theta.$$

Therefore

$$X = R - \frac{d}{2}\sin 2\theta + \alpha \sin\theta + \beta\cos\theta - O\left(\frac{1}{R}\right).$$

We now want to find the length OC. We consider

$$|OC|^2 = X^2 + Y^2 = X^2 + O(1) = \left(X + O\left(\frac{1}{X}\right)\right)^2,$$

so that

$$|OC| = X + O\left(\frac{1}{X}\right) = R - \frac{d}{2}\sin 2\theta + \alpha\sin\theta + \beta\cos\theta - O\left(\frac{1}{R}\right).$$

This is our radial polar coordinate r. The direction of the vector OC is the angle $\pi/2 - \theta - \gamma$, i.e.

$$\Theta = \frac{\pi}{2} - \theta - \gamma.$$

Now the maximum size of γ has

$$|\sin\gamma| \leq \frac{d}{2R\cos\phi} = O\left(\frac{1}{R}\right),$$

so therefore

$$\gamma = O\left(\frac{1}{R}\right).$$

Hence we have

$$\Theta = \frac{\pi}{2} - \theta + O\left(\frac{1}{R}\right).$$

A.2 Replacing Θ by θ

We saw in (8.7) of chapter 8 that

$$\frac{\mathrm{d}\Theta}{\mathrm{d}\theta} = -1 + O\left(\frac{1}{R}\right). \tag{A.3}$$

This is found straightforwardly from our expression $\Theta = \pi/2 - \theta + O(1/R)$ but we check here using partial derivatives of (A.1). From (A.1) we have

$$r\cos\Theta = R\cos\phi\sin\theta + \frac{d}{2}\cos\theta$$
$$r\sin\Theta = R\cos\phi\cos\theta + \frac{d}{2}\sin\theta.$$

We take the partial derivative of these expressions with respect to θ, to get

$$\frac{\partial r}{\partial \theta}\cos\Theta - r\sin\Theta\frac{\partial \Theta}{\partial \theta} = R\cos\phi\cos\theta - \frac{d}{2}\sin\theta \quad ①$$
$$\frac{\partial r}{\partial \theta}\sin\Theta + r\cos\Theta\frac{\partial \Theta}{\partial \theta} = -R\cos\phi\sin\theta + \frac{d}{2}\cos\theta. \quad ②$$

Then ②$\cos\Theta$ − ①$\sin\Theta$ gives

$$\begin{aligned} r\frac{\partial \Theta}{\partial \theta} &= -R\cos\phi\sin\theta\cos\Theta - R\cos\phi\cos\theta\sin\Theta \\ &\quad + \frac{d}{2}\cos\theta\cos\Theta + \frac{d}{2}\sin\theta\sin\Theta. \end{aligned}$$

Since $\Theta = \pi/2 - \theta + O(1/R)$, we see that $\sin\theta$ and $\cos\theta$ are equal to $\cos\Theta$ and $\sin\Theta$ respectively up to acceptable error terms. We have

$$\begin{aligned} r\frac{\partial \Theta}{\partial \theta} &= -R\cos\phi\sin^2\theta - R\cos\phi\cos^2\theta + O(1) \\ &\quad + \frac{d}{2}\cos\theta\sin\theta + \frac{d}{2}\sin\theta\cos\theta + O(d/R) \\ &= -R + \frac{d}{2}\sin 2\theta + O(1). \end{aligned}$$

We then divide by r, and use $r \approx R$ so that

$$\frac{\partial \Theta}{\partial \theta} = -\frac{R}{r} + O\left(\frac{1}{R}\right) = -1 + O\left(\frac{1}{R}\right).$$

Also ①$\cos\Theta$ + ②$\sin\Theta$ gives

$$\begin{aligned} \frac{\partial r}{\partial \theta} &= R\cos\phi\cos\theta\cos\Theta - R\cos\phi\sin\theta\sin\Theta + \frac{d}{2}\cos\theta\sin\Theta - \frac{d}{2}\sin\theta\cos\Theta \\ &= -R\cos\phi\cos(\theta+\Theta) - \frac{d}{2}\sin(\theta-\Theta). \end{aligned}$$

Again we use $\Theta = \pi/2 - \theta + O(1/R)$, and then

$$\begin{aligned} \frac{\partial r}{\partial \theta} &= R\cos\phi\cos\left(\frac{\pi}{2} + O\left(\frac{1}{R}\right)\right) - \frac{d}{2}\sin\left(2\theta - \frac{\pi}{2} + O\left(\frac{1}{R}\right)\right) \\ &= O\left(\frac{1}{R}\right) + \frac{d}{2}\cos\left(2\theta + O\left(\frac{1}{R}\right)\right) \\ &= O(1). \end{aligned}$$

We therefore have a Jacobian determinant of

$$\begin{vmatrix} 1 & 0 \\ O(1) & -1 + O\left(\frac{1}{R}\right) \end{vmatrix} = -1 + O\left(\frac{1}{R}\right).$$

We want to find the area using our polar coordinates. By our estimate for the Jacobian, we can replace the differential of area $r\,\mathrm{d}r\,\mathrm{d}\Theta$ by

$$\int\int r\left(-1 + O\left(\frac{1}{R}\right)\right)\,\mathrm{d}r\,\mathrm{d}\theta,$$

between appropriate limits. As Θ runs from 0 to $\pi/2$, so θ runs from $\pi/2$ to 0, so we have

$$\begin{aligned}
\int_0^{\frac{\pi}{2}}\int r\,\mathrm{d}r\,\mathrm{d}\Theta &= \int_{\frac{\pi}{2}}^0\int r\,\mathrm{d}r\,\mathrm{d}\theta\left(-1 + O\left(\frac{1}{R}\right)\right) \\
&= -\int_{\frac{\pi}{2}}^0\int r\,\mathrm{d}r\,\mathrm{d}\theta + O\left(\frac{1}{R}\left|\int_{\frac{\pi}{2}}^0\int r\,\mathrm{d}r\,\mathrm{d}\theta\right|\right) \\
&= \int_0^{\frac{\pi}{2}}\int r\,\mathrm{d}r\,\mathrm{d}\theta + O\left(\frac{1}{R}\left|\int_{\frac{\pi}{2}}^0\int r\,\mathrm{d}r\,\mathrm{d}\theta\right|\right).
\end{aligned}$$

We then used our limits for r in chapter 8 to begin the integration and area estimation, and to simplify the order of magnitude term to get

$$\int_0^{\frac{\pi}{2}}\int r\,\mathrm{d}r\,\mathrm{d}\Theta = \int_0^{\frac{\pi}{2}}\int r\,\mathrm{d}r\,\mathrm{d}\theta + O(1).$$